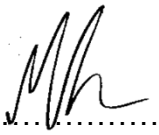
Wallop Primary School

Data Protection Policy - 2023

Produced By:	M. Lambert, Headteacher
Approved for School: Headteacher: M Lambert Date:	 ……(Signature)
Approved by Governing Body: Chair/Deputy Chair: N Slater Date:	 ……(Signature)

General Data Protection Regulation

Our Commitment:

The School is committed to protect all personal and sensitive data for which it holds responsibility as the Data Controller and to handling such data in line with the data protection principles set out in the Data Protection Act (DPA).

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Changes to data protection legislation (including the General Data Protection Regulation that came into force on the 25th May 2018) will be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows:

(a) Consent: the member of staff/pupil/parent/carer has given clear consent for the School to process their personal data for a specific purpose;
(b) Contract: the processing at the School; and
(c) Legal obligation: the processing is necessary for the School to comply with the law (not including contractual obligations).

The members of staff responsible for data protection are:

- Martin Lambert (Headteacher);
- Mai Talbot-King (School Administration and Finance Officer); and
- Charlotte Evans (School Administrator).

The School has identified **Charlotte Evans** as the Data Protection Officer (DPO).

However, all staff must treat all pupil and staff information in a confidential manner and follow the guidelines set out in this policy.

The School is also committed to ensuring that its staff are aware of this Data Protection Policy and legal requirements and that adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the School and any third party contracted to provide services within the School.

Notification:

The School's data processing activities will be registered with the Information Commissioner's Office (ICO) as a recognised Data Controller. Details are available from the ICO:

https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken will be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data will be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the School's control shall be identified as personal, sensitive or both so as to ensure that it is handled in compliance with legal requirements and so that access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data are those published by the ICO for guidance:

https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed so as to:
- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary;
- process the data in accordance with the data subject's rights;
- ensure that data is secure; and
- ensure that data is not transferred to other countries without adequate protection.

Fair Processing/Privacy Notice:

The School will be transparent about the intended processing of data and communicate their intentions via notifications to staff, parents, carers and pupils prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the School is required, either by law or in the best interests of its pupils or staff, to pass information on to external authorities, for example local authorities, Ofsted or the Department of Health and Social Care. These organisations are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within notifications which will detail the basis for sharing. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them.

Under no circumstances will the School disclose information or data:

- that would cause serious harm to the child, or anyone else's, physical or mental health or condition;
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child;
- recorded by a pupil in an examination;
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the School or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed; or
- that is in the form of a reference given to another school or any other place of education or training, or any national body concerned with pupil admissions.

Data Security:

In order to assure the protection of all data being processed and to inform decisions on data processing activities, the School will undertake an assessment of the associated risks of the proposed processing as well as the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. The nominated data protection staff shall be responsible for the effectiveness of the controls implemented and reporting on their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of their competence in their security controls for shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by the School have a legal right to request access to such data or information about what is held. The School will respond to such requests within one month of receipt. All requests should be made in writing to:

Martin Lambert
Headteacher
Wallop Primary School
School Lane
Nether Wallop
Stockbridge
SO20 8EH

No charge will be made by the School for processing the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless the School is obliged by law to do so or it is in the best interest of the child.

Notwithstanding the above, data may be disclosed to the following third parties without consent:

- **Other schools**
  If a pupil transfers from the School to another school, their academic records and other data that relates to their health and welfare will be forwarded on to the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move;

- **Examination authorities**
  This may be for registration purposes, to allow the pupils at the School to sit examinations set by external exam bodies;

- **Health authorities**
  Where obliged under health legislation, the School may pass on information regarding the health of children in the School so as to monitor and avoid the spread of contagious diseases in the interest of public health;

- **Police and courts**
  If a situation arises where a criminal investigation is being carried out, the School may have to forward information on to the police to aid their investigation. The School will pass information on to courts as and when it is ordered to do so;

- **Social workers and support agencies**
  In order to protect or maintain the welfare of pupils at the School or in cases of child abuse, it may be necessary to pass personal data on to social workers or support

agencies;

- **Educational division**
  The School may be required to pass data on in order to help the government to monitor the national educational system and to enforce laws relating to education; or

- **Right to be Forgotten:**
  Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and that all their personal data is erased by the School, including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in the School only.

Unless prior consent from parents/carers/pupils/staff has been given, the School will not utilise such images for publication or communication to external organisations.

It is also the School's policy that external parties (including parents and carers) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:

Hard copy of data, records, and personal information will be stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the School day. This will be held securely by the School Administrator.

Sensitive or personal information and data will not not be removed from the School site. However, the School acknowledges that some staff may need to transport data between the School and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on School visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the School site. If these were to be misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the School site, the information should not be on view in public places, or left unattended under any circumstances;
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name;
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers;
- If information is being viewed on a PC, staff must ensure that the screen and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers;

- If it is necessary to transport data away from the School, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computer. Work should be edited from the USB, and saved onto the USB only; and
- USB sticks that staff use must be password protected.

These guidelines will be clearly communicated to all School staff and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The School recognises that the secure disposal of redundant data is an integral element of the compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf

The School has identified a qualified source for disposal of IT assets and collections.

The School also uses Shred-it to dispose of sensitive data that is no longer required.

Review:
This policy will be reviewed on an annual basis