General Data Protection Regulation Policy
Wilby CE VA Primary School

School Commitment:

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

Changes to data protection legislation (General Data Protection Regulations May 2018) shall 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 has given clear consent for the school to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for the member of staff's employment contract or pupil placement contract.

(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

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.

Roles:

The member of staff responsible for data protection, the Data Controller, is the Head Teacher. The Head Teacher may delegate data controller duties as necessary.

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

The Data Protection Officer (DPO) is Ruth Hawker, Plumsun Ltd. Contact details can be found

on the website: www.plumsun.com

The DPO monitors internal compliance, and informs and advises the school about their data protection obligations and acts as a contact point for data subjects and the supervisory authority.

The DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level.

All staff will treat all pupil information in a confidential manner and follow the guidelines as set out in this document.

Any Data Processors, processing data on behalf of the school (i.e. external organisations) will confirm that they are achieving their obligations under the GDPR Regulations, and are registered with the ICO.

Roles under GDPR can be found on the ICO Website.

Training:

The school is also committed to ensuring that staff are aware of data protection policies, legal requirements.

Notification:

Data processing activities and persons responsible will be registered with the Information Commissioner's Office (ICO) as required by the ICO. 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 shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified to the individual(s) concerned and the ICO as specified in the GDPR Regulations.

Personal and Sensitive Data:

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

The definitions of personal and sensitive data shall be those published by the ICO for guidance.

Principles:

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

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.

The need for consent:

The school will ask for consent to hold and process personal information if there is no lawful basis for doing so:

1) Contract
2) Legal Obligation
3) Vital Interests
4) Public task
5) Legitimate

If personal information meets the above criteria, then individuals who have personal information held by the school will be made aware of the personal information and the criteria for holding the information in the 'Information Audit' document, located on the school website.

Data Breaches:

All data breaches must be immediately reported to the Data Controller (Head Teacher).

The Data Protection Controller will assess whether the breach needs to be reported to the ICO and/or individuals concerned.

The Data Controller will make any necessary reports.

Immediate Action will be taken to review how the breach has occurred, and to make any necessary changes to procedures to ensure that the same problems do not arise in the future.

The Data Protection Officer will provide a monitoring role and be a contact point for the

supervisory authority as necessary.

Protection Impact Statements:

The school will evidence the thought and decision making process about data protection when designing any processes in school which involve personal data.

A Data Protection Impact Statement (DPIA) is needed when:

- New Technology is being deployed
- A profiling operation is likely to significantly affect individuals
- There is processing on a large scale of the special categories of data ('special categories' as specified in GDPR guidance)

Individuals Rights:

Individuals have the right to:

- Be informed about what data is being held (Information Audit Document published on the school website).
- Be informed about how and why the data is being processed (Information Audit Document published on the school website).
- The right to access any data that is being held (see Subject Access Requests below).
- The right to request that any data is erased (see Subject Access Requests below).
- The right to restrict processing.
- The right to data portability (that the individual can transport the data held about them to another service) if the data is held by automatic means.
- The right to object to the way data is being held or processed.
- The right not to be subject to automated decision-making.

The individual can write to the Head Teacher regarding requests for data to be erased, to restrict processing, to data portability, to not be subject to automated decision-making, or the right to object to the way data is being held or processed.

Sharing of Information with Third Parties:

There may be circumstances where the school is required either by law or in the best interests of pupils or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities have to adhere to data protection law and have their own policies relating to the protection of any data that they receive or collect.

Personal data about children, will not be disclosed to third parties without the consent of the child (at an age who can act for themselves, specified under GDPR guidance) the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Examples of data that may be disclosed to third parties without the need for consent:

- Other schools If a pupil transfers from one school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.

- 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 (under health legislation), the school may pass on information regarding the health of children in the school 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 we may have to forward information on to the police to aid their investigation.

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

- Department for Education and Ofsted to help the government monitor and audit school performance and enforce laws relating to education.

The intention to share data relating to individuals to an organisation outside of the school shall be clearly defined within notifications and details of the basis for sharing given. These details are provided in the 'Information Audit Document' located on the school website. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information, or where it is for the purpose of pupil provision, such as school meals and on-line curriculum work.

Any proposed change to the processing of individual's data shall be notified to them (see the 'Information Audit Document' above). 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
- 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.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by the school, has a legal right to request access to such data or information. A child may make a subject access request for themselves, specified under GDPR guidance. The school shall respond to such requests within one month.

They should be made in writing to the Head Teacher, who may delegate the request (as specified in their role above).

The Data Protection Officer (specified in 'Roles' above) will independently advise any requests as necessary. They will acts as a contact point for data subjects and the supervisory authority.

No charge will be applied to process the request.

There is a right to appeal to the ICO upon dispute of a decision.

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 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 school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of Information and Data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information, attendance registers and signing in books (which must be immediately accessible and used in the case of an emergency). Sensitive or personal information and data should 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. Risks of identified breaches from existing processes have been considered and have been recorded on an Impact Assessment Form.

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, unless the Data Controller has provided permission to do so (such as the need for emergency information during educational visits). If there is no other 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 window 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 password protected USB stick or computer. Computers will also be encrypted if it viable to do so. The data should not be transferred from computers or USB onto any public computers. Work should be edited from the USB, and saved onto the USB or authorised computers only.

These guidelines are 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 Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally 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 and in compliance with the Data Protection Regulations (GDPR).

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of 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 the competence in the security of shared data.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to 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.

Abbreviations:

GDPR – General Data Protection Regulations
ICO - Information Commissioners Office
DPR – Data Protection Officer

Approved by:

Dated:

Written by: Ruth Hawker, Plumsun Ltd
Data Protection Officer on behalf of the School/Trust

Dated: 16th March 2018