



# **Wharton CE Primary School**

Greville Drive, Winsford, Cheshire, CW7 3EP

## **Appropriate Policy Document**

DRAFT

<b>Document Control Information</b>	
Document ID	APD01
Document title	Appropriate Policy Document
Version	1.0
Status	Draft, subject to Governing body approval
Author	Martin Bell
Publication date	16 <sup>th</sup> December 2020
Next review date	by School Governors

<b>Version History</b>			
<b>Version</b>	<b>Date</b>	<b>Detail</b>	<b>Author</b>
1.0	16/12/2020	Draft Policy – subject to Governor Approval	Martin Bell Data Protection Lead

<b>Approvals</b>	
<b>Approver</b>	<b>Date</b>

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

When processing personal data, the school will comply with the requirements of the EU General Data Protection Regulation (2016/679 (EU GDPR), the Data Protection Act 2018 (DPA) and any associated legislation.

This Appropriate Policy Document will cover all processing of special category personal data carried out by Wharton CE Primary School for which all of the following conditions are met:

- we (data controller) are processing personal data which is the subject of Articles 9 or 10 of EU GDPR.
- we (data controller) are processing this personal data in reliance of a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA.
- the condition listed in Parts 1, 2 or 3 of Schedule 1 includes a requirement for the data controller to have an Appropriate Policy Document.

Schedule 1 Part 4 of the Data Protection Act 2018 provides additional safeguards that must be implemented when processing information relating to the following types of data:

#### **Part 1 – Conditions relating to employment, social security and social protection.**

- Processing personal data concerning health in connection with our rights under employment law.
- Processing data relating to criminal convictions under Article 10 EU GDPR in connection with our rights under employment law in connection with recruitment, discipline or dismissal.

#### **Part 2 – Substantial Public Interest Conditions**

##### **Statutory etc. and government purposes**

- Fulfilling the school's obligations under UK legislation for the provision of educational services.
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.

##### **Equality of opportunity or treatment**

- Ensuring compliance with the obligations under legislation such as the Equality Act 2010.
- Ensuring we provide equal access to our services, in recognition of our legal and ethical duty.

##### **Preventing or detecting unlawful acts**

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the school and the community.

##### **Protecting the public against dishonesty etc.**

- Processing data concerning dishonesty, malpractice or other improper conduct in order to protect the local community.
- Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Assisting other authorities in connection with their regulatory requirements.

##### **Preventing fraud**

- Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

### **Support for individuals with a particular disability or medical condition**

- To provide services or raise awareness of a disability or medical condition in order to deliver appropriate services and educational support.

### **Counselling**

- For the provision of confidential counselling, advice or support or of another similar service provided confidentially.

### **Safeguarding of children and individuals at risk**

- Protecting vulnerable children and young people from neglect, physical, mental or emotional harm.
- Identifying individuals at risk.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

### **Safeguarding of economic well-being of certain individuals**

- To protect the economic wellbeing of an individual at economic risk who is aged 18 or over.
- Data sharing with our partners to assist them to support individuals.

### **Insurance**

- Information that is necessary for insurance purposes

### **Disclosure to elected representatives**

Assisting elected representatives such as local government Councillors and Members of Parliament with requests for assistance on behalf of their constituents.

### **Part 3 – Additional Conditions Relating to Criminal Convictions, etc.**

Extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.

- We may process personal data relating to criminal convictions or offences in connection with its statutory functions or as part of recruitment and employment checks.

### **Procedures for securing compliance within Article 5 of the General Data Protection Regulation and Data Protection Act 2018**

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

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up-to-date
- retained for no longer than necessary, and
- kept secure

In addition, Article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

Our Data Protection Policy sets out requirements for the data protection principles to be complied with when processing personal data. Our Data Protection Officer ensures that the data protection principles are applied and that we can be held accountable for the personal data it processes.

When processing special category data, the following procedures are used to ensure compliance with the data protection principles:

**Principle a - lawful, fair and transparent**

- Personal data shall be processed lawfully, fairly and in a transparent manner. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.
- We will:
  - Provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.
  - Ensure that personal data is only processed where a lawful basis applies.
  - Will ensure that data subjects are not misled about the purposes of any processing.

**Principle b - collected for specific and legitimate purposes**

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

**Principle c - adequate, relevant and limited to what is necessary**

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- We collect personal data necessary for the relevant purposes and ensure it is not excessive.
- The information we process is necessary for and proportionate to our purposes.
- Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.
- We will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.
- Will employ the use of Data Protection Impact Assessments to ensure proposed processing is not excessive.
- Where possible, anonymisation or pseudonymisation are used.

**Principle d - accurate and, where necessary, kept up-to-date**

- Personal data shall be accurate and, where necessary, kept up to date.
- We will take particular care to do this where our use of the personal data has a significant impact on individuals.
- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.
- If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

**Principle e - retained for no longer than necessary**

- Personal data shall be 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.

- We will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.
- We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.
- Retention periods are based on legal requirements to retain data and consideration of the needs of data subjects through data protection impact assessments.
- Our retention schedule is reviewed regularly and updated when necessary.
- Retention periods are set out in our Retention and Disposal Schedules and are published in our Records of Processing Activities Register and Privacy Notices

### **Principle f – integrity and confidentiality (security)**

- Personal data shall be 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.
- We will ensure that there appropriate organisational and technical measures in place to protect personal data.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation are used to reduce the risk of sensitive data being compromised.
- Hard copy information is processed in line with our security procedures.
- The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

### **Accountability principle**

In order to demonstrate compliance with the Accountability Principle, We have implemented the following measures:

- We keep a record of all our personal data processing activities
- We carry out a Data Protection Impact Assessments
- We have appointed a Data Protection Officer
- We have in place internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law
- All employees receive annual data protection and information security training
- We undertake regular data protection audits
- We maintain logs of security incidents, data protection rights requests and details on information sharing with partners

### **Retention and destruction of personal data**

- Personal data is held and disposed of in line with our Record Retention and Disposal Schedules.
- When disposing of information, we make sure this is carried out securely by using physical destruction methods as well as electronic data deletion.
- Our Record of Processing Activities register contains details of the retention periods for our data processing activities, together with information on the lawful basis for processing this data. If information is not retained or deleted in line with the policy then the reason is recorded in the Record of Processing Activities.

### **Responsibility for the processing of special category and criminal data**

All employees are required to comply with our policies when processing personal data and to ensure that any processing of the personal data is carried out legally, fairly and transparently. Senior staff are responsible for ensuring that systems and processes under their control comply with current data protection legislation and that personal data is processed in accordance with the data protection principles

### **Further information**

For further information about our compliance with data protection law, please contact the Data Protection Officer by:

Email: [schooldpo@cheshirewestandchester.gov.uk](mailto:schooldpo@cheshirewestandchester.gov.uk)

By post: Wharton CE Primary School, Greville Drive, Winsford, Cheshire, CW7 3EP.

DRAFT