Wharton CE Primary School

Greville Drive, Winsford, Cheshire, CW7 3EP

Staff Data Protection Policy

Policy Version Control			
Author	**Summary of changes**	**Version**	**Authorised & Date**
Data Protection Officer	Revision of policy	V0.1	
M Bell (Data Protection Lead)	Reviewed for School	V1.0	Draft for Governor Approval

Policy Management & Responsibilities	
Owner	This policy is owned by the Data Protection Lead on behalf of Wharton CE Primary School. The Data Protection Lead has the authority to issue and communicate policy on legal and statutory compliance including related priorities. Wharton CE Primary School has delegated responsibility for the day-to-day management, implementation and communication of the Policy to the Data Protection Officer.

Policy Review	
Review due:	Annually by school Governors
Document Location:	Secure school data storage and school website

1. Legal Framework

1.1 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

1.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- All Article 29 Working Party Guidance on the implementation of GDPR

1.3 This policy will be implemented in conjunction with the following other CWR documents:

- Add additional policies here

2. Purpose and Scope

2.1 Wharton CE Primary School's Data Protection Policy is produced for a number of key purposes and is intended to be read by staff that handle personal data.

2.2 It gives an overview of how data protection applies to all school staff. It tells staff how data protection applies to their day to day work and areas of data protection that they must be aware of.

2.3 This policy gives practical advice to staff about what to do in specific situations, such as receiving a rights request, discovering a potential data breach and to comply with data protection when handling personal data.

2.4 It makes staff aware of the school's commitment to data protection compliance and tells staff where to obtain further advice and information where necessary.

2.5 This policy has been approved by Wharton CE Primary School's Board of Governors. Any breach of this policy will be taken seriously and may result in disciplinary proceedings.

2.6 Any individual who considers that the policy has not been followed in respect of their personal data should raise the matter with the school's Data Protection Officer, in the first instance. It is a mandatory requirement to report any serious data breaches to the Information Commissioner's Office within 72 hours. These should be reported immediately to schoolDPO@cheshirewestandchester.gov.uk

3. Data Protection Definitions

3.1 For the purpose of this policy:

3.2 Personal data refers to information that relates to an identified or identifiable, living individual (Data Subject), including an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.3 Sensitive personal data is defined in the GDPR as 'special categories of personal data', which includes the processing of personal data revealing;

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- data concerning health
- sex life or sexual orientation

3.4 Processing Data is referred to throughout the GDPR and data protection legislation. This means any use of the personal information. This includes collecting, disclosing, destroying, archiving and organising. This policy applies to both automated personal data and to manual filing systems.

3.5 Data Subject is the person who the personal data is about. For example, the workforce members named on a timesheet are all data subjects of that register.

3.6 Data Controller is usually an organisation who dictates the reason and purpose for how data is processed. CWR itself is a Data Controller as it chooses how it collects, uses and shares its own data. Wharton CE Primary School's registration number is ZA142741.

3.7 The Information Commissioner's Office (ICO) is the regulator for Data Protection and Privacy law in the UK. They have the power to enforce on organisations for breaches of the Data Protection Act or the GDPR. This means they can issue: -

- An Undertaking which commits an organisation to improving their Data Protection practices.
- An Enforcement Notice ordering that an organisation does something specific e.g. train all staff to a high standard.
- A Monetary Penalty for serious and significant breaches. Under the General Data Protection Regulation this can be up to €20 Million or 4% of a company's global turnover.

4. The Principles of Data Protection

4.1 Data protection is a principle-based law, meaning that there are a number of guiding principles that the school must meet in order to comply. These principles guide how we handle personal data and each principle must be met completely.

4.2 The data protection principles state that personal data shall be:

- Processed fairly, lawfully and in a transparent way.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary, kept up to date.
- Kept for no longer than is necessary.
- Kept secure.

4.3 The GDPR also includes a responsibility for the school to document and demonstrate how it complies with the law.

5. How the Principles Apply

5.1 Wharton CE Primary School has a responsibility to ensure that its staff are aware of the data protection principles and ensure they are followed at all times. Data protection applies to all types of personal data held by the school, whether they are paper based or electronic and whether the data relates to staff, parents, pupils, visitors or any other individual who interacts with the school.

5.2 Principle 1 – Fair, Lawful and Transparent

5.2.1 Transparent

5.2.1.1 When using personal data, the school must be open and clear about what the data will be used for and how it will be used.

5.2.1.2 The GDPR requires the school to provide a wide range of information to the person whose data we are using. This is done through Privacy Notices (sometimes called Privacy Policies).

5.2.1.3 The school produces a number of privacy notices that detail how we process the personal data of staff, pupils and parents.

5.2.1.4 The school will ensure all application forms, surveys and contact forms have an accompanying Privacy Notice, whether they are online or in paper form. The school's current privacy notice is available on the school website.

5.2.1.5 Our Privacy Notices must be clearly and plainly written, be communicated to the person whose data we are collecting at the earliest possible opportunity and contain the following information: -

- The name and contact details of the organisation that will own their data (usually the school).
- The purposes we will use their personal data for.
- The school's lawful basis (see more below) for using the personal data.
- How the individual can change their mind or opt-out of their data being used.
- The types of personal data we will use about them (e.g. – their name, their date of birth and their nationality).
- Who we will share the information with and/or who within the school will be able to access it.
- How long we will keep the data for.
- How their data is stored securely.
- Whether their data will be transferred abroad.
- Whether their data will be used to make any automated decisions about them or used to profile them.
- What rights the individual has over the use of their data.

- How to complain about the use of their data, both internally to the school's Data Protection Officer or to the Information Commissioner's Office.

5.2.2 **Fair and Lawful**

5.2.2.1 The school must always ensure its use of personal data is both fair and lawful.

5.2.2.2 Fair means that we must consider whether our use of personal data may affect individuals and consider any adverse impact on them. It also means that we are open and honest with them through our Privacy Notices about how their data is used.

5.2.2.3 Lawful means that the school does not use personal data for any unlawful purposes and that personal data is not used to break either data protection or any other law of the land. This could include a breach of confidence, the Human Rights Act or copyright.

5.2.2.4 Lawful also requires the school to identify a legal basis within the GDPR for its use of personal data. The GDPR contains six lawful bases. One of them must be applied to every function that requires the use of personal data.

5.2.2.5 The lawful bases are:

- Consent – The individual has given their clear agreement for the school to use their data for the purpose.
- Contract – The use of personal data is necessary for a contract we have with the individual or steps we are taking to enter into a contract with them.
- Legal Obligation – The use of personal data is necessary for the school to comply with the law. This could be a statutory obligation or a court order.
- Vital Interests – The use of personal data is necessary to protect someone's life. This is usually a life or death situation.
- Public Task – The use of personal data is necessary to provide a task in the public interest or is in line with a power in law that the school has.
- Legitimate Interests – The use of personal data is necessary to support the legitimate interests of the school or a third party. This condition also states that the school must not use information in this way if it will compromise the rights or freedoms of the person who the data is about.

5.3 **Principle 2 – Collected for a Specific Purpose**

5.3.1 The school must ensure that it collects personal data for clear, appropriate and legitimate purposes. Collecting personal data "just in case" for future reference is not compliant with the legislation.

5.3.2 Through our Privacy Notices we must communicate our purposes to individuals when we collect their data in a clear way.

5.3.3 Whilst the GDPR state the school must only use personal data for the purposes we specify, it may also re-use that data for compatible purposes.

5.4 **Principle 3 – Adequate, Relevant and Limited to what is Necessary**

5.4.1 The school must only use, collect or share personal data in a proportionate way. This means that it should collect what it needs to complete its purposes but nothing more than that.

5.4.2 The school will periodically review the data it collected to ensure it is only collecting data that is necessary.

5.5 **Principle 4 – Accurate and Up to Date**

5.5.1 Personal data must be accurate and up to date. Inaccurate information is one of the key contributors to data protection incidents. Without accurate information, the school cannot complete a wide range of key functions.

5.5.2 Collecting inaccurate data is an automatic breach of the GDPR. Where inaccuracies are identified, they must be rectified as soon as possible and as many steps taken as possible to ensure the correct information is updated on school systems.

5.5.3 Staff are required to double-check what they enter into school systems and emails.

5.5.4 When collecting new information about an individual, they must ensure that their record is kept up to date so that all staff that have access to the data can view the most current details.

5.6 **Principle 5 – Kept No Longer Than Is Necessary**

5.6.1 Personal data must only be kept for a specific period of time. This time period will vary depending on what purpose the personal data is collected for. The school's Retention Schedule details how long personal data should be kept for each function.

5.6.2 Some computer systems operated by the school will automatically delete data when it reaches its deletion date. The majority will not. This means that staff need to be proactive in reviewing what data is held and how long it needs to be kept for.

5.6.3 Where possible, staff are encouraged to use anonymisation or pseudonymisation techniques to depersonalise the data they hold. This will provide a greater level of GDPR compliance.

5.6.4 Personal data held for research and archiving purposes is largely exempt from retention, where this is the only purpose for holding it. However, this data cannot be re-used for another purpose or to make decisions that affect the individuals the data is about.

5.7 Principle 6 – Stored Securely

5.7.1 The GDPR states that the school must take appropriate "technical and organisational" measures to keep the personal data that we hold in a secure way. This does not only apply to personal data held electronically, it also applies to physical documents that hold personal data.

5.7.2 We must ensure that our systems have confidentiality, integrity and availability, and that they can be restored in the event of a system outage.

5.7.3 Keeping personal data secure can be done in a range of ways, often a combination of technical and organisational measures will be used to provide the maximum level of security.

5.7.4 Some examples of technical measures

- Firewalls.
- Anti-virus software.
- Encrypted devices.
- Password protection.
- Access based controls to systems.
- Confidential waste bins.
- Regulated access to buildings.
  Some examples of organisational measures

5.7.5 Policies and procedures that give staff information about handling personal data.

- Data protection training.
- Increased staff awareness and appropriate culture around data protection.
- Guidance notes for staff.
- Written contracts with system providers and other organisations that hold personal data on behalf of the school.
- Periodic audits and reviews of data protection practices.

6. The Rights of the Individual

6.1 Under data protection legislation, all individuals have a range of rights they can use to understand how their personal data is used by the school or exert an amount of control over how it is used.

6.2 One of the rights is the right to be informed. This is covered in the Fair and Transparent section. The Rights include:

- The Right of access (often called Subject Access Requests) – an individual has a right to see a copy of the personal data held about them by the school and find out what it is used for.
- The Right of rectification – an individual can request that inaccurate information held about them is either rectified or deleted.
- The Right of erasure (Right to be forgotten) – an individual may ask for their personal data to be deleted by the school
- The Right of restriction – an individual may ask that the use of their data is restricted whilst a complaint regarding its use is dealt with.
- The Right of data portability – an individual may ask for certain types of their data to be transferred directly to another organisation.

- The Right to object – an individual has the right to stop their personal data being used for certain purposes. This applies to direct marketing through calls and emails.
- Rights over automated decision making and profiling – an individual has the right to stop automated decisions being made about them and ask for human intervention instead. The school does not currently make any automated decisions using personal data.

6.3 Although the rights of the individual are a key foundation of how data protection works, the rights are not absolute. For example, the Right of Access is subject to numerous exemptions and the other rights only apply in certain situations and to certain types of data.

6.4 General Rules Around Rights Requests:

- A request can be made verbally or in writing.
- The school will need to identify the person making the request and verify who they are.
- The school must respond to rights requests within 30 days of receipt.
- The school cannot charge the individual for their response.

6.5 **What to do if you receive a Rights Request**

6.5.1 Rights requests are generally received directly by the Data Protection Lead. However, they can be made to any member of staff. It is important that all staff know what to do if they receive a request and act quickly so the response is not delayed.

6.5.2 Rights requests must be forwarded immediately to the Data Protection Lead.

6.5.3 Rights requests will often not state they are a Rights request specifically. They can come in as part of conversations with students, parents, staff or members of the public. Often, they come in as part of complaints.

6.5.4 The individual does not have to state that they "wish to use their right of access under the GDPR". If any individual asks to see the information the school holds about them, this is Subject Access Request.

6.5.5 If you are unsure whether the correspondence you have received is a Rights Request, send it the DPO for assessment and completion.

7. Data Protection Incidents and Breaches

7.1 It is important that all staff are aware of data protection and what to do in the event of a data breach. Under Principle 6, examples of technical and organisational measures used to keep personal data secure were detailed. It is important that the school has as many of these measures in place as possible.

7.2 When investigating a data protection issue, it is important that a clear distinction is made between an "incident" and a "breach".

7.3 The Information Commissioner's Office is the regulator for data protection in the UK and has the power to levy fines and other enforcement measures on organisations that suffer serious breaches. These fines are for measures that aren't taken to stop incidents from

happening.

7.4 Further examples of data protection incidents include (but are not limited to):

- Emails sent to the wrong recipients.
- Letters sent to the wrong address.
- Documents lost or misplaced.
- Information collected from individuals without a privacy notice.
- Inaccurate information entered onto school systems.

8. Staff Responsibilities around data protection incidents

8.1 Regularly review policies, procedures and security measures around how data is stored, collected and shared. If any gaps are identified, inform the Data Protection Officer and ask for advice. This can help prevent future incidents.

8.2 Report any incident, no matter how minor you believe it to be, to the Data Protection Officer. Minor incidents can not only escalate but can also be used to identify trends in weaknesses in the school's data protection approach.

8.3 Handle personal data with respect at all times. All staff should handle personal data responsibly and take professional pride in ensuring its security and integrity.

9. Responsibilities under this Policy

9.1 Head Teacher/Head of Governors

- To oversee and promote an appropriate data protection culture within the school.
- To provide a view on contentious data protection issues raised within the school.

9.2 Data Protection Officer

- To advise individuals within the school over the use of personal data and compliance with the law.
- To oversee compliance measures and ensure the school complies with the law as far as possible.
- To liaise with the Information Commissioner's Office over serious data breaches.
- To oversee and promote an appropriate data protection culture within the school.

9.3 Individual Members of Staff

- To handle personal data in a responsible and appropriate way.
- To report data protection incidents and risks to the school's data protection compliance to the Data Protection Officer as soon as possible.
- To forward Rights requests to the Data Protection Lead as soon as possible upon receipt.
- To use school systems and communications tools (including email) in a professional manner at all times.

10. Policy Compliance

10.1 Failure to comply with this Policy and associated guidance in protecting school information (or that entrusted to us by a third party) puts the school at risk of reputational damage as well as a breach of legal and regulatory requirement. It may also lead to

disciplinary action in accordance with the relevant Disciplinary Policy (staff or student) or misconduct investigation in accordance with relevant Misconduct Policy.

10.2 Where staff members deliberately or maliciously remove, destroy or sell personal data belonging to the school, the incident will be reported to the Information Commissioner's Office and dealt with through the school's disciplinary process.

10.3 The DPA contains numerous criminal offences for deliberate misuse of personal data. Where a member of staff has committed an offence of this nature, the school will pursue this offence as far as possible.

11. Data Protection Tips for Staff

- Using personal data in a safe and secure way does not need to be complicated. All staff are reminded to follow the points below and refer to this policy first or ask for advice from the Data Protection Officer if they are unsure of how to proceed.
- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left onscreen.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
- Double check when entering information into systems. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Once the email has gone, it cannot be retrieved. Take the time to get the recipient right before you press send.
- When taking information out of the office, think about the most appropriate way to do so. School tablets and laptops are encrypted and difficult to access if they are lost. Paper documents are not as secure as they can be read by anyone who finds them.
- If you don't need to print something, don't.
- If you are regularly sending personal information to organisations outside of the school, ensure that you verify who you are contacting and password protect the document if necessary.
- Where possible avoid using names and other identifiers in email subject headings and meeting/calendar requests.
- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. You wouldn't leave your own laptop on the front seat of your car, so don't leave your work one there either.

12. Using School Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate work purpose to access information
- Never share passwords. If a colleague forgets their password, they need to have it reset by IT. Do not let them access a system under your username.

- Any information you access on a system will be logged. Do not let colleagues use your computer to retrieve information and do not undertake requests on their behalf.
- Always be professional when using school systems. Do not input anything derogatory, inappropriate or rude about individuals.

13.Who to Contact

If you need further advice about data protection, please contact:

Martin Bell, Data Protection Lead.