Data Breach Policy 2020 - 2021

Wylye Valley
Primary School

Love Care Respect

To aspire to being outstanding in everything we do, by always aiming higher.

"Let your light shine in all you say and do."

Matthew 5:16

Status	**Recommended/Statutory**
Approval Date and by	
Review Frequency	**Annual**
Effective From	
Review Due	
Committee	
Data Protection Officer	**Mr Jeremy Shatford** **Dpo@jeremyshatford.co.uk**

1 Policy Statement

1.1 Wylye Valley School processes personal information about its pupils, parents, staff, volunteers, and other individuals who we deal with. This can include sensitive information ("Special Category Data").

1.2 By complying with our own internal data protection procedures, we recognise that in the event of a data breach, it is critical that we have effective response procedures in place to minimise the impact on those affected.

1.3 This procedure applies to all school staff, governors, volunteers, and contractors.

1.4 A personal **data breach** under the UK-GDPR or the **Data** Protection Act 2018;

1.4.1 A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. It is therefore important to recognise that a data breach is not just the loss of personal information.

1.5 Examples of data breaches include the following:

(a) Loss or theft of personal data and / or equipment on which data is stored.
(b) Sending personal information to the incorrect recipient.
(c) Unauthorised access of personal information.
(d) Hacking.
(e) Cyber-attack.
(f) Accidental destruction.

1.6 The above list is not exhaustive. If you are in any doubt as to whether a data breach has occurred or not, you should err on the side of caution and report it in accordance with this procedure.

2 Reporting the Breach and Immediate Steps

2.1 Any person who has caused a data breach, discovers a data breach, or is informed of the occurrence of a data breach, must immediately notify the Headteacher. If the Headteacher is unavailable, then a member of the Senior Leadership Team (SLT) should be contacted. A form to assist with the initial fact finding is available here.

2.2 The Headteacher or the member of the SLT must immediately report the data breach to the DPO by telephone (07881 297319) or email (mailto:dpo@jeremyshatford.co.uk).

2.3 If, in the opinion of the DPO, the data breach is likely to result in a risk to the rights and freedoms of those affected, the Chair of Governors should be notified.

2.4 The DPO, along with the headteacher, will be responsible for assessing the data breach and advising the school on any immediate action that it may need to take to address any risks arising. In doing so, the DPO will consider the following:

(a) Is the data breach still occurring?
(b) If the answer to (a) is yes, then immediate steps must be agreed to minimise the breach from continuing.
(c) Consideration should be given to notifying the police if the breach was caused by, or suspected to have been caused by, unlawful activity (e.g. hacking). The police should also be notified if the breach may lead to unlawful activity in the future (e.g. if bank details have been lost in human error, this could lead to fraud in the future).
(d) Any third parties who may be affected by the breach should be notified. This could include the relevant local authority departments (e.g. Children Services) and service providers.

(e) If the nature of the breach is such that it may result in media or press enquiries, those responsible for handling such enquiries should be notified. The DPO will also assist with any information to be provided to the media.
(f) ICT technicians at the school and / or third-party ICT providers should be consulted, if appropriate, to advise on any security measures that can be put in place to minimise the impact of the breach e.g. shutting down systems, changing passwords, retrieving lost data.
(g) Where bank details have been lost or stolen, banks should be contacted to assist them in responding to any potentially fraudulent activity.

3 Investigation

3.1 The DPO must immediately support the school in investigating the data breach reported, taking such steps as are reasonable to identify the following: -

(a) When the breach occurred.
(b) The factual background relating to the breach.
(c) Who has been affected by the breach e.g., staff, parents or pupils?
(d) The number of people affected by the breach.
(e) The type and sensitivity of the data concerned.
(f) The consequences or potential consequences of the breach.
(g) The measures put in place to minimise the breach.

3.2 The investigation should be completed urgently as its findings will inform whether the Information Commissioner's Office ("ICO") and/or data subjects need to be informed.

4 Record of Breach

4.1 The breach must be recorded in the Data Breach & Near Miss Log.

5 Notification of a Data Breach to the ICO

5.1 The DPO will aim to report to the ICO not later than 72 hours after the School became aware of the breach using the ICO online reporting tool. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

5.2 If a notification to the ICO is made, the DPO will ensure that appropriate steps are taken to fully co-operate with their requests / investigations.

6 Notifying the Data Subject(s)

6.1 If the data breach is likely to result in a high risk to the rights and freedoms of the data subject(s) the DPO will ensure that steps are taken by the School to notify where appropriate the data subjects without delay.

7 Post Breach Procedure

7.1 It is imperative that regardless of how serious or minor the breach, lessons are learnt, and measures are put in place to avoid a similar incident occurring again in the future.

7.2 The measures put in place should be proportionate to the breach. However, such measures could include the provision of further training, introduction of new policies and procedures or changes to security measures.

7.3 The Headteacher will report the findings of the investigation at the next Governing Body meeting including the measures introduced to avoid any future breaches.