St Mary's C of E (VA) Primary School

To be a caring, inclusive, Christian environment, nurturing a life-long love of learning where we can work together to learn, to grow, to serve. We are proud to support the whole community and by collaborating will enable all children and adults within it to live fully whilst 'shining brighter and brighter' Proverbs 4:18.

St Mary's is an inclusive school where we believe that all people are of equal value, irrespective of their ethnicity, culture, religion, gender, ability or sexual identity. We recognise and respect their differences.

GDPR Data Breach Procedure Policy

This policy is GDPR compliant.

Date of issue: November 2020
Last reviewed/adopted: November 2020 (Resources Committee)
Next review date: Autumn 2022

Signed:_____ Date:_____

The school has robust processes in place to minimise the risk of data breaches. In the event of a data breach, we will notify the ICO (Information Commissioner's Office) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. The school has appointed a Data Protection Officer (DPO) in accordance with GDPR requirements. The DPO will investigate and review any reported data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to the DPO, via the Deputy DPO (both individuals are identified in the Data Breach Log) with immediate effect, whereby the procedures detailed in this policy and school GDPR folder are followed. You can contact the school's Data Protection Officer at admin@stmary's916.herts.sch.uk.

A data breach is described as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also notify those concerned directly. All breaches, regardless of severity, will be recorded within the Data Breach Log. Changes to procedure or policy may result after a review of each breach by senior staff and the DPO.

How will we identify a breach?

- Teaching and admin staff will be annually trained to strengthen their understanding of GDPR and data breaches, including information on who to report to and when.
- Staff should report concerns directly to a member of Senior Leadership Team (SLT) and the Deputy DPO (identified within the Data Breach Log) who will inform Data Protection Officer as necessary.

How will a breach be handled?

- The Deputy DPO will meet with key staff to make a decision as to whether there has been a data breach.
- The Deputy DPO will inform the DPO if a breach is suspected.
- The DPO (or Deputy DPO if unavailable) will report the data breach to the ICO if required. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority, in accordance with Article 33 of the GDPR.
- The school will report the breach to the data subject(s) concerned where necessary, in accordance with the GDPR.
- The Deputy DPO will record the reported breach in the Data Breach Log.

How will a breach affect future data control?

- The Data Protection Officer will propose any necessary changes to procedure in order to mitigate future data breaches of this kind.
- In the event of human error, re-training and/or disciplinary measures will be employed as appropriate. The individual concerned may be removed from compliance related tasks.
- In the event of a system error, IT support staff, senior staff and the DPO will liaise to identify the cause and take appropriate action to prevent a repeat of the breach.
- Changes in policy and/or procedure will be documented as necessary.
- Staff will be trained in changes to policy and procedure.

Data Privacy Impact Assessment (DPIA)

A PIA will be carried out in situations of high risk such as:

- where a new technology is being deployed.
- where a profiling operation is likely to significantly affect individuals.
- where there is processing on a large scale of the special categories of data.
- PIAs provided by suppliers will be stored in the Supplier Compliance Evidence folder or a link will be added within the Supplier Compliance Log.

Record Keeping

- Any Data Breach Logs will be kept for a period of 6 years from the date of the incident.
- The Data Protection Officer checks processes and controls every term and a logs of Data Risk, Data Breaches, Subject Access Requests are maintained by the school and subject to inspection and interrogation during the termly DPO visits.