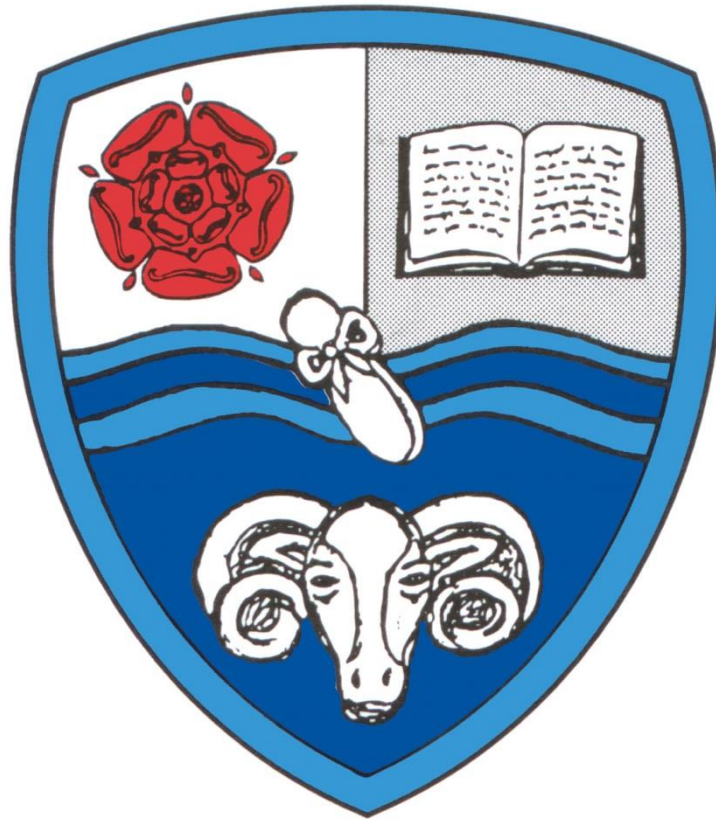


St Mary's CE Primary School, Rawtenstall

Data Breach Procedure



Data Protection Policy Statement

- St Mary's Primary School processes a significant amount of personal information about our pupils, parents, staff, governors, volunteers and other individuals who we come into contact with. This can include sensitive information.
- By complying with our own internal data protection procedures, and through promoting a strong culture of data protection compliance, our aim is to avoid the occurrence of a data breach. However, 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.
- The General Data Protection Regulation (GDPR) also places reporting obligations on the school, as data controller, in the event of a data breach. This procedure has been implemented to ensure that appropriate action is taken in a timely manner to comply with the requirements of GDPR.
- This procedure applies to all school staff, the governing body, volunteers and contractors.

Identifying a Data Breach

- 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.
- Examples of data breaches include the following:
 - Loss or theft of pupil, staff or governing body data and/or equipment on which data is stored.
 - Sending personal information to the incorrect recipient
 - Unauthorised access of personal information
 - Hacking
 - Cyber-attack
 - Accidental destruction
- 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.

Reporting the Breach and immediate steps

- Any person who has personally caused a data breach, discovers a data breach, or is informed of the occurrence of a data breach, must immediately notify the school bursar – Mrs Helen Collinge. If the school bursar is unavailable, then the Headteacher (Mr Neil Gurman) should be notified directly.
- If in the opinion of the DPO (Mr Neil Gurman), 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.
- The school should immediately contact the DPO with a view to agreeing immediate steps to address the breach. The following should be considered:
 - Is the data breach still occurring?
 - If the answer is yes, then immediate steps must be agreed to minimise the breach from continuing.
 - 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).

- Any third parties who may be affected by the breach should be notified. This could include the relevant local authority departments (e.g. Children's Services) and service providers.
- 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 to allow them to prepare for such enquiries.
- 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.
- Where bank details have been lost, banks should be contacted to assist them in responding to any potential fraudulent activity.

Investigation

- The DPO must immediately support the school in investigating the data breach reported, taking such steps as are reasonable to identify the following:
 - When the breach occurred
 - The factual background relating to the breach
 - Who has been affected by the breach e.g. staff, parents or pupils
 - The number of people affected by the breach
 - The type and sensitivity of the data concerned
 - The consequences or potential consequences of the breach
 - The measures put in place to minimise the breach
- 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.

Record of Breach

The breach should be recorded in the Data Breach Record.

Notification of a Data Breach to the ICO

- As appropriate, the DPO will ensure that a data breach is reported to the ICO not later than 72 hours after the school became aware of the breach using the letter template at appendix 1.
- Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.
- If the data breach is unlikely to result in a risk to the rights and freedoms of those affected by the breach, then the notification to the ICO will not be necessary.
- A data breach is likely to result in a risk to the rights and freedoms of those affected by the breach if it causes a loss of control over the personal information or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality. These examples are not exhaustive and the breach must be assessed on a case by case basis by the DPO.

- 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.

Notify the Data Subject(s)

- 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 the data subjects without delay using the letter template at appendix 2.
- Those affected by the data breach need not be notified if any of the following apply:
 - The school had implemented appropriate technical and organisational measures, and those measures were applied to the personal information affected by the data breach, in particular, those that ensure the personal information is unintelligible to any person who is not authorised to access it, such as encryption and the data is recoverable e.g. as it was backed up.
 - The school has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise.

Post Breach Procedures

- 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.
- 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.
- Where the breach was notified to the Chair of Governors in accordance with the Headteacher will report the findings of the investigation at the next Governing Body meeting including the measures introduced to avoid any further breaches.

Policy written by Mr N Gurman – Headteacher and DPO

Approved by the Governing Body – February 2022

Next review date – February 2023



St Mary's CE Primary School Rawtenstall

Headteacher: Mr N Gurman
T: 01706 216407

E: head@rawtenstall-st-marys.lancs.sch.uk

W: www.stmaryscep.org.uk

Appendix 1

The Information Commissioner's Office

[Insert Address 1]

[Insert Address 2]

[Insert Address 3]

Date

Dear Sirs,

Notification of a Data Breach in accordance with Article 33 of the General Data Protection Regulation (GDPR)

We write to the Information Commissioner's Office in accordance with Article 33 of the GDPR to provide notification of a data breach. It is considered that the breach is notifiable on the basis that it is likely to result in a risk to the rights and freedoms of those affected.

[We are aware that notification should be made to the ICO by no later than 72 hours after having become aware of the data breach. Unfortunately, we were unable to comply with this requirement for the following reasons xxxxxx].

The nature of the data breach, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

[insert details]

Name and contact details of the DPO

**Mr Neil Gurman
Headteacher
St Mary's CE Primary School
Unity Way
Haslingden Old RD
Rawtenstall
BB4 8RZ**

The likely consequences of the data breach

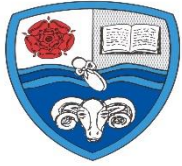
[insert detail]

Measures taken or proposed to be taken by the school to address the breach

[insert detail]

We look forward to your office contacting us shortly

Yours sincerely



St Mary's CE Primary School Rawtenstall

Headteacher: Mr N Gurman

T: 01706 216407

E: head@rawtenstall-st-marys.lancs.sch.uk

W: www.stmaryscep.org.uk

Appendix 2

The Information Commissioner's Office

[Insert Address 1]

[Insert Address 2]

[Insert Address 3]

Date

Dear xxxx

Notification of a Data Breach

We write to you to advise of a recent data breach within the school. Having considered the nature of the breach, we have reported this to the Information Commissioner's Office who will advise us the next steps in their process. The ICO is the UK's independent body set up to uphold information rights.

The purpose of this letter is to provide you with information about the data breach, how it occurred, who it has affected, the type of information which the breach relates to, the consequences of the breach and the measures we have taken to address the breach.

Details of the breach

INSERT DETAIL

Name and contact details of the DPO

Mr Neil Gurman
Headteacher
St Mary's CE Primary School
Unity Way
Haslingden Old RD
Rawtenstall
BB4 8RZ

The likely consequences of the data breach

[insert detail]

Measures taken or proposed to be taken by the school to address the breach

[insert detail]

Clearly, we appreciate that you will be concerned about the data breach described within this letter. On behalf of the school, we sincerely apologise for any distress that this may cause. We can assure you that we are taking all necessary steps to address the situation. Should you wish to discuss this with the Data Protection Officer, then please feel free to do so by telephone on 01706 216706 or email – head@rawtenstall-st-marys.lancs.sch.uk



Loving, Learning,
Community.

Yours sincerely