St John the Baptist RC Primary School

Data Breach Procedure

Policy Statement

1.1 St John the Baptist RC Primary School ("the School") processes a significant amount of personal information about its pupils, parents, staff, volunteers and other individuals who we come into contact with. This can include sensitive information ("Special Category Data").

1.2 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.

1.3 The UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR") also places reporting obligations on the School, as a 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 the GDPR.

1.4 This procedure applies to all School staff, trustees, volunteers and contractors.

2. Identifying a Data Breach

2.1 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. Staff are referred to the HYin5ive data protection series for a refresher on what constitutes a data breach (https://hyeducation.co.uk/blog/)

2.2 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.

2.3 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.

3. Reporting the Breach and Immediate Steps

3.1 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 Headteacher. If

the Headteacher is unavailable, then the Data Protection Officer ("DPO") should be notified directly.

3.2 The Headteacher must immediately report the data breach to the DPO by telephone (0161 543 8884) or email (DPO@wearehy.com).

3.3 The DPO 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 (non-exhaustive list):

(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.

4. Investigation

4.1 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.

4.2 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.

5. Record of Breach

The DPO will record the data breach in the Data Breach Record.

6. Notification of a Data Breach to the ICO

6.1 Subject to 6.3, and providing the School notifies the DPO in a timely manner, 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. The DPO may use the letter template at appendix 1 for this purpose.

6.2 Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

6.3 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 described at 6.1 will not be necessary.

6.4 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 their 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.

6.5 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.

7. Notifying the Data Subject(s)

7.1 Subject to 7.2, 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. The DPO may use the letter template at appendix 2 for this purpose.

7.2 Those affected by the data breach need not be notified if any of the following apply:-

(a) 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.

(b) The School has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

8. Post Breach Procedure

8.1 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.

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

APPENDIX 1

The Information Commissioner's Office
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[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 DETAIL]

Name and contact details of the DPO
HY Education Solicitors Limited
Sandbrook House,
Sandbrook Way Rochdale
OL11 1RY
DPO@wearehy.com

The likely consequences of the data breach

[INSERT DETAIL]

Measures taken or proposed to be taken by the School to address the data breach

[INSERT DETAIL]

We look forward to your office contacting us shortly.

Yours faithfully,

For and on behalf of

APPENDIX 2

[Name]
[Insert Address 1]
[Insert Address 2]
[Insert Postcode]

[Date]

Dear XXXX

Notification of a Data Breach

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

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 Data Protection Officer ("DPO")
We have an appointed DPO who is actively working with the School to address the data breach and their contact details are as follows:-

HY Education Solicitors Limited
Sandbrook House,
Sandbrook Way, Rochdale
OL11 1RY
DPO@wearehy.com

The likely consequences of the data breach

[INSERT DETAIL]

Measures taken or proposed to be taken by the School to address the data breach

[INSERT DETAIL]

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 DPO, then please feel free to do so by telephone on 0161 543 8884 or email DPO@wearehy.com

Yours sincerely,

For and on behalf of