St Gabriel's C of E Primary School

Data Breach Management Policy

April 2018

DATE APPROVED BY COFE PRIMARY SCHOOL	To be approved in Summer Staffing and Community Governing Body Meeting		
REVIEW DATE Biennial	Spring 2019 This policy will normally be under a two yearly review, but with the introduction of the Data Protection Act 2019 following Brexit, the review period has been shortened in the first instance.		
SIGNED HEAD TEACHER		**DATE**	
SIGNED CHAIR OF Governors		**DATE**	

Contents

Source of this policy:

This procedure has been written in reference to the Key's model Data Breach Policy and is based on guidance on personal data breaches produced by the Information Commissioners Office (ICO).

Actions to take should a breach occur:

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer, John Pearson-Hicks john.pearson-hicks@london.anglican.org
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed

  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a locked cupboard as a hard copy in the GDPR file in the head's office and on the Senior Administrators computer in an electronic GDPR file
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO

  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on an electronic spread sheet on the Senior Administrators computer and in a locked file in the head's office.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Details of pupil premium interventions or other interventions for named children being published on the school website

- As soon as the breach is discovered information will be taken down immediately and the DCO informed
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- The DPO will contact the ICO

Non-anonymised pupil exam results or staff pay information being shared with governors

- As soon as the breach is discovered the DCO will be notified
- Governors will be asked to delete any email or electronic copy of the data and the IT technician will recall the email
- Governors will be asked to return any hard copies of the data to the school for shredding

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- No sensitive information is to be stored on portable laptops, tablets or memory sticks unless it is encrypted with strong passwords
- If any data has been stored in a non-encrypted format prior to the introduction of this Data Breach Policy and the Data Protection Policy and there is a breach the Data Controller will contact the DCO immediately and an investigation commence.

Hard Copies of sensitive data going home by accident in homework or in a book bag

- Family receiving the data asked to return it straight away
- DC contacts DPO

- DPO determines if ICO should be contacted

Hard copies of pupil data (including test results, medical data, ethnicity being left on photocopier or printer)

- Person discovering this to inform the Data Controller (Headteacher) the then DC to contact the DPO immediately
- Hard copies to be shredded