LITTLE PLUMSTEAD CHURCH OF ENGLAND VA PRIMARY SCHOOL

DATA BREACH RESPONSE POLICY

This policy has been based on the model policy provided by the DOP Centre Ltd and should be read in conjunction with the school's General Data Protection Regulation (GDPR) and Data Protection Policy.

INTRODUCTION

This policy is designed to ensure that the employees of Little Plumstead Church of England VA Primary School (the School) can identify data breaches and meet the requirements of Data Protection Legislation in the handling of a personal data breach (henceforth "personal data breach" or "data breach"). For reference purposes the School's Data Protection Officer (DPO) is Alison Jones of DPO Centre Limited.

Data Protection Legislation means the Data Protection Act 2018 which incorporates the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the General Data Protection Regulation which is the governing legislation that regulates data protection across the EEA. This includes any replacement legislation coming into effect from time to time.

A personal data breach is defined within the Data Protection Legislation 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". Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental actions by a controller or processor or their employees, agents or contractors;
- human error affected personal data
- sending personal data to an unauthorised recipient;
- network intrusions
- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- alteration of personal data without permission;
- loss of availability of personal data

The notification requirements associated with data breaches rest on the level of risk to the rights and freedoms of data subjects arising from the breach. Unless a personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned data subjects, it is to be reported to the ICO or relevant supervisory authority. Where such data breaches are likely to result in a high risk to the rights and freedoms of the concerned data subjects, the affected data subjects are to be informed in addition to the supervisory authority.

The Data Protection Legislation further stipulates that where notification of the supervisory authority is required, this should take place within 72 hours of the controller becoming aware of the personal data breach. In the case of breaches which pose a high risk to data subjects, the additional requirement to notify data subjects must be done as soon as possible and without undue delay.

In light of these requirements, this policy focuses on the responsibilities of all employees of the School in internally reporting breaches and the external notification requirements.

DEFINITION OF TERMS USED WITHIN THIS POLICY

a. Any reference to "Article" or "Articles" is a reference to an Article or Articles of the "GDPR".
b. The terms 'personal data', 'data subject', 'processing', 'pseudonymisation', 'controller', 'processor', 'recipient', 'third party', 'consent', 'personal data breach', have the meanings set out in Article 4 of the GDPR.

c. "Security incident" means an incident in which the security of personal data may have been compromised but no risk is identified in respect of the rights and freedoms of data subjects. Security incident in the context of this policy may also be used to define an event or action which may compromise the confidentiality, integrity or availability of systems or data, where such event or action does not presently amount to a reportable data breach.

BREACH DETECTION AND REPORTING

A personal data breach or security incident may be detected by any individual who accesses or interacts with systems, records and information belonging to or in the possession of the School. As such, all employees, contractors and processors of the School are responsible for reporting any suspected or actual security incident or data breach.

All security incidents and data breaches, suspected or actual must be reported to the School's DPO via the Headteacher or School Office Manager immediately upon detection. This includes any incidents or data breaches detected outside normal working hours.

When reporting a security incident or personal data breach, suspected or actual, the school's Personal data Breach Procedure will be followed (Appendix 1). The reporter is obliged to disclose all information within their knowledge using the Breach Report Form annexed to this Policy (Appendix 2).

Employees, contractors and processors of the school must report all incidents, including those resulting from human error and those with unidentified or unknown affected data subjects as soon as detected.

BREACH INVESTIGATION

The School, with the assistance of the DPO when appropriate, aims to complete a preliminary investigation of all reported incidents without undue delay. The School aims to establish its awareness of a personal data breach within the first 24 hours of internal detection. Awareness can be established once it is determined that the reported security incident involves personal data which may be compromised as a result of the security incident. From this point, there are 72 hours within which to identify whether there is a risk to the concerned data subjects and where there is a risk, notification to the supervisory authority should take place.

During the initial investigation, the School aims to establish the following:

The facts of the security incident
The data or records concerned
The value and sensitivity of the data or records concerned
The type of breach suspected (confidentiality, availability, integrity)
The number and identity of affected data subjects
The likely consequences of the breach
The measures required to contain the impact of the breach

NOTIFICATION TO THE SUPERVISORY AUTHORITY

All personal data breaches which pose a risk to the rights and freedoms of data subjects will be reported to the Information Commission's Office (ICO). The School's DPO aims to ensure all such notifications are made within 72 hours of becoming aware of the personal data breach.

All notifications to the ICO must be made with the authorisation of the Headteacher and the School's DPO and will be made using the breach notification form provided by the ICO.

COMMUNICATING HIGH RISK DATA BREACHES

Where a high risk to the rights and freedoms of data subjects is established, the School's DPO will inform data subjects of the personal data breach as soon as possible and without undue delay. Communication to data subjects should include:

The nature of the breach
The name and contact details of the DPO or other contact person
The likely consequence of the breach
The measures taken or proposed to be taken by the controller to address the breach
Any recommended steps to be taken by the data subjects themselves e.g. changing passwords.

The School's DPO aims to notify data subjects of relevant personal data breaches directly unless it is impossible to do so, or it would involve a disproportionate effort, in which case the breach may be communicated by way of a public statement. All such communications must be authorised by the Headteacher and DPO.

ACCOUNTABILITY
All security incidents reported will be documented regardless of whether the breach was notifiable to the ICO. The School will maintain a breach register containing all reported incidents (Appendix 3).

Drawn up by:	School Office Manager
Approved by Governors:	Spring 2019
Review date:	Spring 2021

APPENDIX 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- 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 on the secure school's server.
- 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 the secure school server.
- 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 actions 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

APPENDIX 2 – BREACH REPORT FORM

Please complete this form if you have detected or been advised of a data breach. It is imperative that you complete this form immediately upon detection and where possible, please advise the Headteacher or School Office Manager of the suspected breach immediately.

Once completed, please either hand the paper copy to or email this form to office@littleplumstead.norfolk.sch.uk

Incident / breach details	
Name of person reporting incident:	
Contact details of person reporting incident:	
Date(s) incident took place:	
Date you detected the incident:	
Place of incident:	
Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed to be affected:	
Approximate number of affected data subjects, if known:	
Approximate number of affected records, if known:	
Any actions taken in response to the incident:	

APPENDIX 3 – PERSONAL DATA BREACH REGISTER

LITTLE PLUMSTEAD CE VA PRIMARY SCHOOL

Breach Register

Prior to completing entries in this Register please refer to the Breach Policy and Procedures to ensure the effective use of the document and to ensure that any breaches reportable to the ICO are actioned accordingly.
(Service providers must notify the ICO of any personal data within 72 hours of detection)

Organisation: Date:

Breach No.	Details of breach						Consequences of breach	Measures taken/to be taken				
	Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data		All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?	If not notified, why not