HORNINGSHAM PRIMARY SCHOOL

Data Breach Policy & Procedure

'Together we learn'

OUR MISSION STATEMENT STATES THAT WE

Aim to provide a Caring Community where children can grow up confidently and happily whilst providing opportunities to develop their potential to the full.

This procedure should be read in conjunction with our policies and/or procedures on, Data Protection and Records Retention.

Status	**Recommended/Statutory**
Author	**Jeremy Shatford DPO**
Approval Date and by	
Review Frequency	**Annual**
Review Due	

Version control			
Version Number	**Date issued**	**Author**	**Update information**
First Document	01/09/2021	J Shatford DPO	

CONTENTS

1 Vision and Values 3

2 Introduction and Purpose 3

3 Policy Statement 4

4 Scope of the Policy 4

5 Definition / Types of Breach 4

6 Information Security Incidents 4

8 Initial Assessment 6

9 Containment and Recovery 6

10 Notification 6

11 Evaluation and response 7

12 Implementation 7

13 Roles and Responsibilities 8

14 Complaints 8

16 Annex A Breach Notification Form 9

17 Annex B Data Protection Officer Assessment 11

1 Vision and Values

1.1 Horningsham Primary School is a maintained school within the Wiltshire Local Authority. Our Mission Statement is that we "Aim to provide a Caring Community where children can grow up confidently and happily whilst providing opportunities to develop their potential to the full".

2 Introduction and Purpose

2.1 Horningsham Primary School collects and uses personal information about staff, pupils, parents, and other individuals who have contact with the school. This information is gathered to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory responsibilities.

2.2 We are the Data Controller and required to be registered, along with the name of our data protection officer (DPO), with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

2.3 Our data protection officer is Jeremy Shatford who may be contacted in writing to the school clearly labelled "Data Protection", or by email to dpo@jeremyshatford.co.uk.

2.4 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018 (DPA) and incorporates the UK General Data Protection Regulation (UK-GDPR), Freedom of Information Act 2000 (FOI) and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically.

2.5 All staff involved with the collection, processing and disclosure of personal data will be made aware of their duties and responsibilities and adhering to the guidelines set out in this policy.

2.6 This policy relates to all personal and sensitive data that can be attributed to a living individual (data subject) held by the school regardless of format; electronic or paper based.

2.7 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

2.8 This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

2.9 All staff should be aware that any breach of the Data Protection Act 2018 or the UK-GDPR might result in Disciplinary Procedures being instigated.

2.10 The school must have in place a framework designed to ensure the security of all personal data during its lifecycle. The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2.11 Personal data is information that relates to a living individual which allows that individual to be identified from that information (or that information with other information likely to come into the organisation's possession).

2.12 Horningsham Primary School is a Data Controller as it determines the purposes, and the way in which personal data is processed.

3 Policy Statement

3.1 The school regards the Act as an important mechanism in achieving an honest, safe, and open relationship with all those with whom it has dealings with, including, its pupils, parents, and employees.

3.2 The aim of this policy is to ensure that the school complies with its legal obligations under the Data Protection Act 2018 and can evidence that we have done so. It also aims to ensure that we:

- Have robust processes in place for dealing with data breaches, saving time and effort.
- Increase levels of trust and confidence by being open with individuals about the personal information we hold.
- Improve the transparency of our activities in line with public policy requirements.

4 Scope of the Policy

4.1 This is not a legal document. It does not confer rights nor override any legal or statutory provisions which either require or prevent disclosure of personal information.

4.2 This document considers the key features of the Act and outlines how the school will take steps to ensure compliance in relation to the security of personal information.

5 Definition / Types of Breach

5.1 For this Policy, data security breaches include both confirmed and suspected incidents.

5.2 "Personal data breach" under the UK-GDPR covers more than just the unauthorised disclosure of personal information. The phrase is defined 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 by the company"

5.3 An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the school's information assets and/or reputation.

6 Information Security Incidents

6.1 An information security incident is a violation or breach of the school's information security policy and associated acceptable use policies or a breach of the IT code of conduct.

6.2 A security incident is an event which causes or has the potential to cause:

- Degraded system integrity.
- Loss of system or information availability.

- Disclosure of confidential information, whether electronic or paper, or any other form including conversation.
- Corruption of information.
- Disruption of activity.
- Financial loss.
- Legal action.
- Unauthorised access to applications.
- Unauthorised access to premises.

6.3 An incident includes but is not restricted to, the following:

- Attempts (either failed or successful) to gain unauthorised access to a system or its data.
- Unwanted disruption or denial of service.
- The unauthorised use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.
- Loss of removable media (USB Stick, Disc etc) and portable equipment (Laptops/Tablet PCs).
- Tampering/attempting to tamper with CCTV cameras or the leaking of unauthorised film footage taken from CCTV equipment.
- Damage to or theft /loss of ICT equipment or confidential / sensitive papers (either manual or electronic).
- Unauthorised access to confidential / sensitive information in any form including receiving information meant for someone else.
- Unauthorised disclosure of confidential / sensitive information in any form to a third party.
- Transfer of information to the wrong person (by fax, email, post or phone).
- The finding of confidential information/records in a public area.
- The unauthorised usage of another user's security credentials.
- Sharing computer ID's and passwords.
- Accessing another individual's personal details without permission.
- Leaving confidential / sensitive information on public display
- Virus outbreak or ransomware attacks.

7 Reporting an incident

7.1 Any individual who discovers a data breach as defined above, is responsible for reporting the data breach and information security incidents immediately to the headteacher and head of administration, who would report it to the Data Protection Officer.

7.2 The School's Data Protection Officer is Jeremy Shatford a certified data protection officer. Reports should be made via email dpo@jeremyshatford.co.uk or telephone 07881297319.

7.3 If the breach occurs or is discovered outside normal working hours, it must be reported as soon staff become aware of it.

7.4 The incident report should include full and accurate details of the incident form, see annex A. and forward to the data protection officer.

7.5 If the report should be made immediately, with as much information that is available and not delayed establishing these details. The school's management and/or the Data Protection

Officer will work to identify and remedy any gaps and reporting should not be delayed while finding missing information.

8 Initial Assessment

8.1 An initial assessment will be made by the DPO in liaison with relevant school staff to establish the severity of the breach and to determine roles and responsibilities in responding to the breach.

8.2 The DPO[1] will advise a suitable course of action and if necessary, prepare a report for the Information Commissioners' Office (ICO) to be submitted within 72 hours of the breach being detected.

8.3 The 72-hour period does not consider non-working days, weekends, and public holidays.

8.4 The ICO will then consider the severity and cause of the breach, along with the DPO's assessment and actions taken so far and offer advice on further action or if warranted initiate an ICO inspection.

9 Containment and Recovery

9.1 The school, advised by the DPO, will firstly determine if the breach is still occurring. If so, appropriate steps will be taken immediately stop the breach and to investigate and assess the risks associated with it.

9.2 The staff designated by the DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment.
- Instigating a search for any lost/mislaid information.
- The use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

10 Notification

10.1 The school, advised by the Data Protection Officer, must decide whether to notify any individuals affected by the Data Breach. It will not always be necessary, or beneficial to do so, but in any cases where there will be a significant risk to the rights or freedoms of the data subject then the subject will normally be notified.

10.2 Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements

[1] Our DPO is well placed to offer advice however the responsibility remains with the data controller (Horningsham Primary School) to comply with the UK-GDPR and DPA.

- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?

10.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the school for further information or to ask questions on what has occurred.

10.4 The school, with advice from the DPO, must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

10.5 The DPO will advise whether the school should make a press release and to be ready to handle any incoming press enquiries.

11 Evaluation and response

11.1 Once the initial incident is contained, the DPO will co-ordinate a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

11.2 The school will notify the DPO of all actions taken in response to the breach and the DPO will keep appropriate records.

11.3 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11.4 The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure, sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

11.5 A report of the incident will be presented to the school's governing body.

12 Implementation

12.1 The Head Teacher should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager or the Head Teacher.

13 Roles and Responsibilities

13.1 Adhering to the Data Protection Act 2018 is the responsibility of every member of staff acting for or on behalf of the school. Subject Access requests fall within the data protection statutory framework and the ability to identify and appropriately handle a request for information is part of every employee's role.

14 Complaints

14.1 If a data subject is not satisfied with our response to a data breach, we ask that they follow the schools complaints procedure.

14.2 If a data subject remains dissatisfied with our response, or the way their request has been handled, they may also raise a complaint with the ICO.

14.3 Should the ICO investigate Horningsham Primary Schools compliance with the data breach, Horningsham Primary School will be required to provide documentation to prove its compliance with the UK-GDPR along with its principles.

14.4 In the unlikely event that the ICO determine a failure by Horningsham Primary School to comply with the reporting requirements of a breach or that the breach was a result of noncompliance with maintaining proper security, the ICO have various consequences that can result including the following:

- Issuing warnings and reprimands.
- Imposing a temporary or permanent ban on data processing.
- Ordering the rectification, restriction, or erasure of data; and
- Suspending data transfers to third countries.
- Issuing of fines.

14.5 If it were found that Horningsham Primary School failed to comply with any of the UK-GDPR principles, and financial penalty would be increased by 4%.

14.6 The data subject would also be able to make representation through the courts to claim compensation within certain circumstances.

15 Contacts

15.1 If you have any enquiries or concerns or would like more information about anything mentioned in this policy, please contact our administration office by telephone on 01985 844342, or email admin@horningsham.wilts.sch.uk. Alternatively, our data protection officer: Jeremy Shatford by Email: dpo@jeremyshatford.co.uk.

15.2 Further advice and information is available from the Information Commissioner's Office, https://ico.org.uk/or telephone 0303 123 1113

16 Annex A Breach Notification Form

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

On becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

You must complete this form as soon as possible and email it to dpo@jeremyshatford.co.uk without delay. Also confirm by telephone 07881297319 that it has been sent. Strict timelines are in place allowing up to 72 hours for the I.C.O to be informed of any reportable breaches.

Name and contact information for person discovering the incident	
Organisation	
Date and time the incident was discovered and or brought to your attention	
Incident date, time and location	
A description of the nature of the personal data breach including, where possible the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.	
Description of what occurred	
Briefly describe how you first discovered the incident or breach	

Does the incident involve paper records, electronic information or both?

What type of media or records do you believe were involved? Paper: letter, office correspondence, pupil files, photocopying etc. Electronic: data file or record, email, device (laptop, iPAD, desktop, personal devices ie. Mobile phone or other hard drives in other equipment) Media: external hard drive, USB key, other electronic devices) Do you know if the device or information was password- protected? Do you know if the device or information was encrypted?
Do you believe personal data about pupils, employees, parents, or anyone else was exposed?
Can you estimate how many people's records were involved?
To the best of your knowledge, has the incident been contained? (That is, has the data leak or loss stopped or is there still potential for additional data to be lost?
Is there any other important or pertinent information that you can think of?

Signed_____**Dated**_____

Print Name:_____ _____

17 Annex B Data Protection Officer Assessment

Jeremy Shatford DPO
dop@jeremyshatford.co.uk
07881297319

To be completed by the DPO

The date and time of the breach (or an estimate);
The date and time you were informed;
Basic information about the type of breach;
Basic information about the personal data concerned;
The facts surrounding the breach;
The effects of the breach;
Remedial action taken.
Outcome

Signed:

J M Shatford
EU Certified DPO

Updated: 31st August 2021 (DPO)