Longmoor

Community Primary School

Together we grow, explore, discover.

Data Breach Policy

DFE:	Non-Statutory	**Category:**	GDPR
Last Reviewed:	February 2025	**Reviewed by:**	Mark Garside (HT)
Status:	ACTIVE		

Version Log		
1.0	Policy creation: MGA	February 2025

DETERMINATION
RESPECT INTEGRITY
VALOUR EXCELLENCE

Contents

1. Introduction 3

2. Responsibilities 3

Data Protection Officer (DPO) 3

GDPR Lead 3

3. Data Breach Procedure 3

Identifying a Data Breach 3

Reporting a Data Breach 3

Assessing and Managing a Breach 3

Notifying the ICO 4

Notifying Affected Individuals 4

4. Preventing Future Breaches 4

Staff Training 4

5. Monitoring and Review 4

Appendix A: Data Breach Report Form 5

1. Reporter Details 5

2. Breach Details 5

3. Breach Impact 6

4. Containment Measures Taken 6

5. Escalation & Notifications 6

6. Follow-Up Actions & Recommendations 7

7. Signatures & Acknowledgement 7

Longmoor Community Primary School is responsible for reviewing and maintaining this policy in line with the school's policy review schedule. The latest version is available to all staff on the school's shared drive in the **GDPR folder**.

1. Introduction

The UK GDPR and the Data Protection Act 2018 mandate that schools protect personal data and respond effectively to data breaches. This policy ensures that Longmoor Community Primary School has robust procedures to handle personal data breaches promptly and in compliance with legal obligations.

Definitions

- **Personal Data**: Information relating to an identified or identifiable individual.
- **Special Category Data**: Sensitive data such as racial or ethnic origin, health information, and religious beliefs.
- **Personal Data Breach**: A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

2. Responsibilities

Data Protection Officer (DPO)

The Chair of Governors, **Mark Rea**, serves as the school's DPO, overseeing data protection compliance. Contact details:

- **Email**: admin@longmoorcps.co.uk
- **Phone**: 0151 521 5511

GDPR Lead

The **School Business Manager** is responsible for breach notifications and ensuring compliance. In their absence, the **Headteacher** assumes this role.

3. Data Breach Procedure

Identifying a Data Breach

A data breach may involve:

- Loss or theft of data or equipment.
- Unauthorized access to personal data.
- Accidental or deliberate data deletion.
- Cyber incidents such as hacking or phishing attacks.

Reporting a Data Breach

All staff must report suspected breaches immediately by:

1. Completing a **Data Breach Report Form** available from the GDPR Lead.
2. Submitting the form to the DPO at **admin@longmoorcps.co.uk**.
3. Refraining from notifying individuals or conducting further investigations; these actions will be managed by the GDPR Lead and DPO.

Assessing and Managing a Breach

Upon notification, the GDPR Lead and DPO will:

- **Contain the breach** to prevent further compromise.
- **Investigate the incident** to determine the scope and impact.
- **Document the breach** in the school's Data Breach Register.

- **Notify affected individuals** if there is a high risk to their rights and freedoms.
- **Report to the Information Commissioner's Office (ICO)** within 72 hours if required.

Notifying the ICO

Breaches posing a risk to individuals' rights and freedoms must be reported to the ICO within 72 hours of detection. The report will include details of the breach, its impact, and remedial actions taken.

Notifying Affected Individuals

If a breach is likely to result in significant harm, such as identity theft or discrimination, affected individuals will be informed promptly with clear guidance on protective measures.

4. Preventing Future Breaches

Post-breach, the school will:

- **Review and enhance security measures** to prevent recurrence.
- **Provide additional training** to staff on data protection practices.
- **Update relevant policies and procedures** to address identified vulnerabilities.

Staff Training

Regular training sessions will be conducted to ensure all staff understand their responsibilities under data protection laws and are equipped to identify and report potential breaches.

5. Monitoring and Review

This policy will be reviewed annually or following any significant data breach incident. Staff are required to acknowledge their understanding and adherence to this policy.

Appendix A: Data Breach Report Form

Longmoor Community Primary School

Data Breach Report Form

This form must be completed **immediately** when a data breach is suspected or confirmed.

1. Reporter Details

Full Name	
Job Title / Role	
Team	
Date of Report	
Contact Number	
Email Address	

2. Breach Details

Breach	**Date**		**Time**	
Discovered	**Date**		**Time**	
Location of Breach				
DESCRIPTION OF INCIDENT				
Type of Data Involved (Tick All That Apply)				
	Personal Identifiable Information (e.g., names, addresses, DOB)		Special Category Data (e.g., health records, ethnicity, religion)	
	Financial Data (e.g., bank details, payroll)		Student Records (e.g., attendance, assessments)	
	Other (Please Specify)			
How was the breach discovered?				

3. Breach Impact

Who is affected by this breach (Tick All That Apply)			
	Pupils		Parents/Guardians
	Staff		External Agencies
	Other (please specify):		

Who is affected by this breach (Tick All That Apply)			
	Identity theft/fraud		Safeguarding risk
	Financial loss		Discrimination or reputational damage
	Other (please specify):		

4. Containment Measures Taken

Immediate Actions Taken to Contain the Breach				
Has the Data Been Recovered?	YES		NO	
Has the Affected Individual(s) Been Informed?	YES		NO	
Are There Any Ongoing Risk?	YES		NO	
If yes, explain:				

5. Escalation & Notifications

Has the Breach Been Reported to the GDPR Lead?	YES		NO	
If yes, DATE		TIME		
Has the Breach Been Reported to the DPO?	YES		NO	
If yes, DATE		TIME		
Has the ICO Been Notified?	YES		NO	
If yes, DATE		TIME		
Has the Breach Been Reported to Any External Authorities?	YES		NO	
If yes, specify:				

6. Follow-Up Actions & Recommendations

What actions are needed to prevent a similar breach in the future?
Additional Notes:

7. Signatures & Acknowledgement

	Signature	Name	Date
Reporter			
GDPR Lead			
DPO			