Brownlow Fold Primary

Together we fly

DATA BREACH

STATEMENT OF PRACTICE

Version Control

Current version	Previous version	Summary of changes made
Jul 2025	Jul 2024	Policy reviewed in consultation with Headteacher.
Jul 2024	Jul 2021	Policy reviewed in consultation with Headteacher.
Jul 2021	Jul 2018	Policy reviewed in consultation with Headteacher.
Jul 2018		Policy downloaded, reviewed and adopted from LA and amended to our format in Jul 18.

DATA BREACH POLICY

Introduction

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.

1. The School is obliged under Data Protection legislation (The General Data Protection Regulation (GDPR) and related EU and national legislation) to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.
2. This policy relates to all personal and special categories (sensitive) data held by the School regardless of format.
3. This policy applies to all staff and students at the School. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the School.
4. 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.

Purpose and Scope

Brownlow Fold School collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

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

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Although Brownlow Fold takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen.

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

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.

Definitions / Types of breach

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Equipment theft or failure
- System failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- 'Blagging' offences where information is obtained by deceiving the School.

Reporting an incident

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred, must notify the School DPO immediately.

   Shane Williams
   Data Protection Officer
   Global Policing Limited
   For Brownlow Fold Primary School
   Email: datarequests@globalpolicing.co.uk
   Web: globalpolicing.co.uk/data
   Tel: 0161 212 1681

   If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
   All staff should be aware that any breach of Data Protection legislation may result in the School's Disciplinary Procedures being instigated.
   A record of the breach should be created using the following templates:
   - Data Breach Incident Form
   - Data Breach Log
   - Evidence Log

2. **Containment:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form:

    - What type of data is involved
    - How sensitive is it?
    - If data has been lost/stolen, are there any protections in place such as encryption?
    - What has happened to the data?
    - What could the data tell a third party about the individual?
    - How many individuals data have been affected by the breach?
    - Whose data has been breached?
    - What harm can come to those individuals?
    - Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment, the DPO should notify the ICO within 72 hours of the identification of a data breach if it is deemed that the breach is likely to have a significant detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

    - The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the School.

7. **Notification to third parties:** the DPO must consider notifying third parties such as the police, insurers, banks 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.

8. **Evaluation:** The DPO should assess whether any changes need to be made to the School processes and procedures to ensure that a similar breach does not occur. A record will be

kept of any personal data breach, regardless of whether notification was required. This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Appendix 1

Information Security Incident
Report Form
All boxes must be completed
To be completed by the person reporting the breach

Name	
Job title	
Department / Section (if applicable)	
Telephone number	
E-mail address	
Date	
What has happened? Please provide as much information as you can about what has happened, what went wrong and how; include a description of the data, eg: format, volume, from which system, and the location of the breach.	
How did you find out about the breach? If you were not the person who originally found there had been a breach, please explain how you found out about it and how they found out about it.	
Was the breach caused by a cyber incident?	

Yes		**No**		**Not yet known**	

When did the breach occur?	Date:		Time:	
What has happened to the information? (Please select all that apply)				
Destroyed		Lost		Stolen	
When was the breach discovered?	Date:		Time:	
Altered		Unauthorised Disclosure		Unauthorised Access	
Other (please give details below)				

Categories of personal data included in the breach (Please select all that apply)			
Basic personal identifiers (eg: name, contact details)		Identification data (eg: usernames, passwords)	
Racial or ethnic origin		Political opinions	
Religious or philosophical beliefs		Trade union membership	
Health		Sexual life or orientation	
Gender reassignment data		Genetic or biometric data	
Financial information		Criminal convictions or offences	
Official documents (eg: driving licences)		Location data	
Other (please give details below)		Not yet known	

How may data subjects could be affected?	
Categories of data subjects affected (Please select all that apply)	

Employees		Pupils	
Parents / Carers		Governors	
Volunteers		Other (please give details below)	

What is the possible impact of the breach on the data subjects?

Has there been any actual harm to data subjects? (If yes, please give details below)					
Yes		No		Not yet known	

What is the likelihood that data subjects will experience significant consequences as a result of the breach? (Please select one option and give further details below)					
Very likely		Likely		Neutral	
Unlikely		Very unlikely		Not yet known	

Have you told the data subjects about the breach?			
Yes		About to or in process of telling them	
No, but they're already aware		No, but planning to tell them	
No, decided not to tell them		Not yet decided whether to tell them	
Seeking advice from DPO		Other (Please give details below)	

Have you told, or are you planning to tell, any other organisations (e.g. police, regulatory body) about the breach? (If yes, please give details below. If you have a crime reference number, please include it)			
Yes		**No**	
Seeking advice from DPO		**Other (Please give details below)**	
What measures have been taken to deal with the breach? (e.g. contacting the person sent in formation in error, auto-erased lost laptop)			
Has the data been recovered? (Please give details - if the breach is due to a misdirected email, include whether you have had confirmation that the recipient has deleted it and whether it was read or unread)			
Yes		**No**	
What measures have been taken / are proposed to mitigate further breaches?			

If there is any further information you think should be considered please include it here.

To be completed by the Data Protection Officer

Form received by DPO	**Date:**		**Time:**			
Was the form received within 24 hours of the breach being discovered?			**Yes**		**No**	
If no, was a reason given? (Please give details below)			**Yes**		**No**	
Is the information on the form complete?			**Yes**		**No**	
If not, what further information is required? (Please give details below)						

Breach reported to SIRO	**Yes**		**No**		**Date**	
Breach reported to Head Teacher	**Yes**		**No**		**Date**	
Breach reported to Chair of Governors	**Yes**		**No**		**Date**	

What measures have been agreed should be taken to deal with the breach?

What measures have been agreed should be taken to mitigate harm caused by the breach?

Have data subjects been told about the about the breach (if not already done by person reporting it)?

Yes		**About to or in process of telling them**	
No, but they're already aware		**No, but planning to tell them**	
No, decided not to tell them		**Other (Please give details below)**	

Does the breach warrant a report to the ICO?	**Yes**		**No**	
If yes, when was the breach reported to the ICO?	**Date:**		**Time:**	
Was report to ICO made within 72 hours?	**Yes**		**No**	
If report was not made within 72 hours, please provide justification for late reporting below.				
What has been identified as the root cause(s) of the breach following investigation?				
What corrective actions have been identified following investigation?				

Action	Target Date	Owner	Date Completed

DPO Sign-off		**Date**	
Head Teacher Sign-off		**Date**	
Date Incident Investigation Closed			

Appendix 2

Request for personal data Form

Request for personal data

All boxes must be completed

To

Details of applicant

Name of applicant	
Job title	
Department and Section	
Full Address	
Telephone number	
e-mail address or fax number	
Investigation reference / Operation Name	
Date	

Details of application

1. This request is made pursuant to the Data Protection Act 1998. I can confirm that this request complies with the following non-disclosure provisions
Section 29 ☐ The data is necessary for the prevention or detection of crime ☐ The data is necessary for the apprehension or prosecution of offenders Section 35 ☐ The data is necessary for the purpose of or in connection with present legal Proceedings ☐ The data is necessary for the purpose of or in connection with prospective legal Proceedings

2. I require the following information
3. Why I require the information
4. What statutory powers does the requester have to demand the information
5. **I can confirm that the information you provide will be held in the strictest confidence and will not be further processed beyond the purpose for which it was requested.** **I have grounds believing that failure to disclose the required information will be likely to prejudice my enquiries and can confirm that the details supplied on this form are, to the best of my knowledge, correct.** **I am aware of the provisions of Section 55 of the Data protection Act 1998, regarding the unlawful obtaining of personal details.**
Signature Print Name