Leominster Primary School
Information security management incident reporting policy

Data Breach Procedure

Introduction

The School, as a Data Controller have a responsibility to ensure that personal and sensitive personal information is kept securely. If anything goes wrong and, for example, data is lost, stolen, misused or inappropriately accessed or released, the School equally has a responsibility to put things right.

All information security incidents must be reported. This enables the School to conduct a full investigation, and to identify areas of weakness and improvements that need to be made. It also enables the School to take a measured decision whether the incident should be reported to the Information Commissioner's Office. If an incident involving personal data (data about an individual person) is reported directly to the Information Commissioner without the School being aware of it, there is an increase in the likelihood of the School being fined by the Information Commissioner. Fines can reach up to £500,000 per breach.

When sensitive information has been put at risk, but has not actually been lost, stolen, misused or inappropriately accessed or released, it is not an incident though it is not good practice. For example, a member of staff taking sensitive information home without authority but returning it safely the next day would have put data at risk. This sort of practice should be reported to line management to deal with, and the School Management Team to monitor and report to the Governors and / or Local Authority as appropriate.

Actions

Actions	Responsibilities and Duties
1	All identified breaches must be reported to the School's Management Team as soon as they are detected. Even where there is some difference of opinion regarding breach, err on the side of caution and report it.
2	If the breach is identified via a complaint, the School will treat the breach in a similar way to the complaints process with response targets. If the targets cannot be met due to the complexities of the investigation, the complainant will be informed and kept updated on progress until their complaint is resolved.
3	A lead officer within the School, (Management Team / Governor), must be appointed who will investigate the breach and establish why it happened and what remedial action is necessary. The investigating officer will keep the Management Team regularly updated on progress if the breach has been reported as a complaint, so that the complainant can be updated as appropriate.

4	The investigating officer will take professional advice from the Local Authority, Legal Services and Samantha Smith, the School's Data Protection Officer. Advice must be sought in a timely way; for example, if an injunction is required to stop information being released that has been sent somewhere by mistake, Legal Services will need to be involved very early on in the case.
5	Upon detecting a breach, it is important to act quickly. In particular it is important to find out the following:- • The extent of the breach • The amount of information involved • The sensitivity of information involved • A timeline of dates and times concerning the incident • The potential for loss or damage to individuals, the School or any other body • What measures need to be taken and how quickly to address:- i. Restoring any lost information to our custody or control ii. Whether to warn people about the loss, including who to warn and when. This may depend on a risk assessment (see below) iii. Whether to report the loss to the Information Commissioner (if it involves personal data) and when to do so iv. Whether to report the loss to the Police Share information at all stages with the Management Team for incident management and reporting.
6	Carry out and document a risk assessment if required for informing those whose data has been breached. Use the letter template in Appendix 1 to inform those affected depending on the outcome of the risk assessment. Any resulting claims for compensation should be referred to the Local Authority / Legal Services / the Insurers.
7	Report the loss of data to the police as required, and notify the Local Authority.
8	Consider convening a meeting as appropriate involving people who are likely to have an active role in remedying the breach or dealing with any of the outside parties involved. Maintain an action plan tasking individuals with assisting the investigation as necessary.
9	Draw up a chronology of the incident.
10	Consider taking statements, formally through an investigatory interview following the disciplinary procedure or informally, from those involved, especially where the quality of evidence may be lost through time or people may not be present for long.

11	If information has been sent to the wrong address, retrieve the information as soon as possible, using the letter template in Appendix 1 or via a home visit as appropriate.
12	Always consider involving the Council's Public Relations team early on and keeping them updated. [IF APPROPRIATE FOR THE SCHOOL]
13	As part of the process of identifying the cause of the breach, try to consider measures that can be put in place to eliminate or reduce the chances of a reoccurrence. Where these are obvious, put them in place straight away; where these would need further discussion, feed them in to the meeting (if any) at 8 above.
14	Where the incident has been treated as a complaint, the investigating officer will draft a response for the complainant and have it reviewed by the Management Team / Governors.
15	Prepare an incident report and include recommendations regarding reporting to the Information Commissioner's Office following the guidance on reporting as set out by the Information Commissioner. Report the incident to the Information Commissioner if the Management Team takes the decision to report, and deal with any subsequent actions arising from reporting. Complete all follow up actions as required
16	Legal Services will be tasked with dealing with any claims for compensation or other legal matters arising from the breach.

Golden rules for reporting and investigating data breaches

A breach must be reported by the school to the ICO within 72 hours.

Observe the following "golden rules":

- Do not keep a breach to yourself, even if you feel there has been no harm arising. Next time – we may not be so lucky
- Do not seek to apportion blame – the main object of this procedure is to close the breach and better ourselves as a result of it. Instances of wilful breach will be few and far between.
- This procedure is not confined to breaches involving personal data only. Any uncontrolled information loss is important.
- Be honest with the facts.
- Be thorough in investigating or assisting with any investigation.

Reviewed By: Headteacher and Governing Body
Review Date: October 2025
Date of Next Review: **October 2027**

APPENDIX 1

Letter to notify that personal data has been breached

I write to you to bring to your attention a breach of the Data Protection Act 2018 that unfortunately involves your personal data.

As you would imagine we have taken this matter very seriously and *are investigating the matter / have concluded our investigation into it.*

The facts in this matter are *<give description of what has happened>.*

<State what remedial action(s) have been carried out>

<State what has been done to prevent a reoccurrence>

If you have any questions or concerns regarding this letter, please get in touch with me *or alternatively speak to your social worker who is aware of the situation*.

I would again like to apologise for the incident of which you were no doubt unaware.

Yours sincerely,

APPENDIX 2

Letter to retrieve information in response to notification by service user

NB: Follow up if no response is received after 10 days with a further letter reminding them to return the letter. If a response is still not received, contact Legal Services for advice.

Thank you for your *letter / telephone call* of *<date>* bringing the incident whereby *<state what has happened>* to our attention. We are obliged to you for acting in such a responsible way in contacting us.

As you would imagine we have taken this matter very seriously and have concluded our investigation into it.

The facts in this matter are *<give description of what has happened>.*

Could you please return the document to me at the address below by <date 10 days from now> so that I can ensure that the document is securely destroyed.

<State what remedial action(s) have been carried out>

<State what has been done to prevent a reoccurrence>