THOMAS JOHNSON LOWER SCHOOL

Hurst Grove, Lidlington, Bedfordshire MK43 0SB
Tel: 01525 402377 / 01525 404743
email: thomasjohnson@cbc.beds.sch.uk

Data Breach Procedure Policy

Responsibility	All staff and the Governing Body
Review Date	May 2019
Approved by Full Governing Body	May 2018
Storage: (i) Electronic (ii) Hard Copy	(i) School website (managed by school secretary) (ii) School staff room

Policy Statement

Thomas Johnson Lower School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Thomas Johnson Lower School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Thomas Johnson Lower School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach (see appendices for examples, forms and guidance)

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Assistant Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. 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. In such instances, advice from the School's legal support should be obtained.
5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.
b. Contacting the relevant Local Authority Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).
c. The use of back-ups to restore lost/damaged/stolen data.
d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
e. 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.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include

a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO 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 the DPO or the Head Teacher.

Appendix A:

Examples of different categories of potential breaches

There are 3 categories of breach. ALL risk occurances start as a potential breach and then are recorded as near miss, potential breach or formal breach. The formal data breach requires recording on the formal data breach log.

"Near miss" example 1

A teacher contacts the Head to say that an envelope containing sensitive personal information about the medical condition of a pupil was given to the wrong parent. The envelope has not be opened. The school will need to collect the envelop to secure the information. In this instance the information was contained. This would be recorded as **a "near miss**". The school would look into how this could be avoided in future.

"Near miss" example 2

A teacher's laptop is damaged after being accidently dropped. The files are backed up and can be recovered. This incident has a lower level of risk as data can be recovered by the school and is not in the public domain (therefore the data subjects would not have suffered damage or distress). In this example the risk can be managed by the school and an apology does not need to be sent. The incident would be logged as a **"near miss**".

"Potential breach" example 1

The school secretary reports that a child's assessment from the Educational Psychologist went to the wrong address. The home owner opened the letter and read the contents before notifying the school. This is **a potential breach** that needs investigating. It cannot be contained because the letter has been opened. This may be referred to the ICO. The safety of the child should also be considered and additional safeguarding procedures may need to be followed (e.g. in the case of a Looked After Child, where disclosure could affect the safety of the child and family).

At the end of the investigation, the decision is reached to tell the data subject so that they can take any steps they feel necessary to protect their personal information, such as from identity theft. The school explains what went wrong and what has been done to remedy the situation and prevent it from happening again.

"Potential breach" example 2

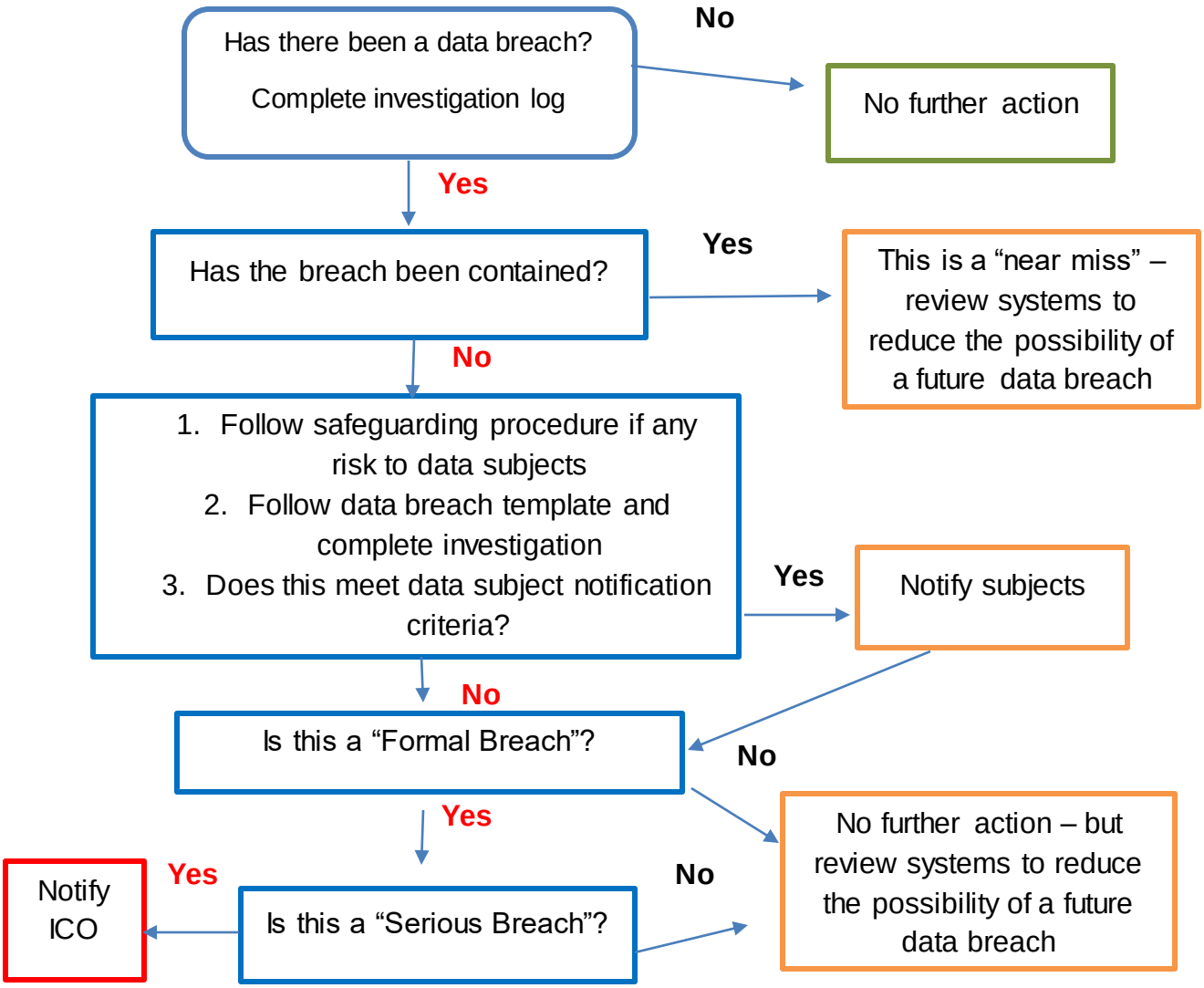
In the previous case of the broken laptop, if data cannot be recovered and the school has to reconstruct the data set, this needs to be logged as a **potential breach**. The investigation will reveal why the data was stored in such a way that it could become corrupted and was not recoverable. If the data subject was not directly affected they do not need to be informed. If they were affected (such as a missed appointment) they would need an apology.

"Formal data breach" example

A spreadsheet with medical assessments including those of vulnerable children was emailed to 400 taxi firms. The breach cannot be contained. It involves sensitive information of more than 5 people. This requires an investigation

Number of people involved	1000+					
	100					
	50					
	5					
	1					
		e.g. Name, address	e.g National Insurance Number	e.g. Bank details, medical information	e.g. Details of a vulnerable child	e.g. Full medical files or criminal file
	Sensitivity of the Information					
Key	**Unlikely to require recommending as a formal breach**		**Consideration should be given to recommending as a formal breach**		**Likely to require recommending as a formal breach**	

Breach flow chart



Reporting a Potential Data Breach

To be completed by the School's Data Protection Officer

Date of Incident		
Date you were made aware of the potential breach		
Location of incident		
Nature of incident	**Loss / theft / disposal / unauthorised disclosure**	
Nature of data involved. List all data elements (e.g. names, files, dates of birth, or reference numbers)		
What security protection was on the data?	**Password / Encryption / Other … (state)**	
Is there a back up of the data?If so where?		
Number of people potentially affected (an estimate should be provided if no precise figure can be given)		
Details of any steps taken to retrieve data or to contain the breach if it involved unauthorised access or potentially compromised security.		
Does an investigation template need completing or can this incident be contained within the school?	**Logged as "near miss"**	**Investigation template completed**
Signature of DPO		

Note: if the incident involved the theft (e.g. a bag containining personal documents or a laptop) the theft must be reported to the Police.

Further Investigation Template - example

Note: Only column B is required to be submitted. Column A acts as a prompt and should be deleted once the form has been filled in.

Column A (delete once form has been filled in)	**Column B**
Prompt sheet	Type your investigation report in this column
Incident date	*Add date*
Incident number	*Add your number*
Author(s) / Invetigating officer	*Name of person*
Report Date	*Date*
Incident description and consequences	*The personal information of 25 vulnerable children was disclosed when an email was sent to parents of children who had left the school*
Information retrieved	*Yes or no*
Decision as to whether those individuals whose data has been breached are to be notified	*The 25 children involved medical records. The individuals concerned have been notified.*
Chronology of events (for complex cases any timeline included in the report should be a summary)	*When discovered, when last use of data, when authority notified, when information recovered if recovered, when data subject informed of risk etc.*
Contributory factors (A list of significant facts)	*Over the years addresses had been added causing the team to lose track of the lists*
Root Causes (These are the fundamental underlying factors contributing to the incident that can be addressed. Root causes should be meaningful (not sound bites such as communication failure) and there be a clear link between root CAUSE and EFFECT.)	*Staff involved had not deleted old lists. Some lists. There is no procedure regarding how long names are kept.*
Lessons learned (Key issues identified which may not have contributed to this incident but from which others can learn.)	*Old email addresses and hard copy telephone numbers are deleted on inset day (start of new term) or as a child leaves.*
Type of breach	*Please tick one of the following:* *Near miss* *Potential breach* *Futher action (Please provide details):*

	No further actions *Formal breach*
Recommendations (Numbered and referenced) Recommendations should be directly linked to root causes and lessons learned. They should be clear but not detailed and kept to a minimum wherever possible. All recommendations are to be Specific, Measurable, Acheivable, Realistic and Timely.	*Ensure all email lists are reviewed on the first inset in Sept so that past information is deleted.*
Arrangements for shared learning (Describe how learning has been or will be shared with staff and other organisations.)	*Share findings with other schools sharing similar activities.*
Outcome (The conclusion of the investigation should state whether the author believes the breach should be logged formally or not)	*As the breach resulted in sensitive personal information being inappropriately shared with more than 10 people it is recommended that this be recorded as a formal data breach.*
Headteacher and Chair of Governors **Date**	

Further Investigation Template

Column A (delete once form has been filled in)	Column B
Prompt sheet	Type your investigation report in this column
Incident date	
Incident number	
Author(s) / Invetigating officer	
Report Date	
Incident description and consequences	
Information retrieved	
Decision as to whether those individuals whose data has been breached are to be notified	
Chronology of events	
Contributory factors	
Root Causes	
Lessons learned	
Type of breach	*Please tick one of the following:* *Near miss* *Potential breach* *Futher action (Please provide details):* *No further actions* *Formal breach*
Recommendations	
Arrangements for shared learning	
Outcome	
Headteacher and Chair of Governors **Date**	