Data Breach Policy 2025-2027

APPROVED AND ADOPTED

Policy Author: Headteacher & School Business Manager
Approved by: Full Governing Body
Approved on: 15th May 2025
Date of issue: November 2022
Review Date: May 2027

DATA BREACH TOOLKIT

Contents **Page**

Hatch Warren Junior School
DATA BREACH POLICY

1. Introduction

This is the school's Data Breach policy which should be read alongside our Data Protection Policy.

To carry out the school's functions it is necessary to process personal data relating to our staff, pupils, parents, visitors and others.

Personal data is information relating to a living individual who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

The personal data the school processes includes special category data this is data which is of sensitive nature such as health information, racial or ethnic origin, biometric data and trade union membership.

2. What is a Personal Data Breach?

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.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

3. What responsibilities does the school have in relation to a personal data breach?

3.1 Notification to the ICO

The school is required by the GDPR to report certain types of personal data breach to the Information Commissioner's Office (ICO).

When a personal data breach has occurred, the school will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's

likely that there will be a risk, then the school must notify the ICO; if it's unlikely then the school doesn't have to report it.

The school must report a notifiable breach to the ICO within 72 hours of becoming aware of the breach, where feasible.

3.2 Communication with the affected individuals

The school is required by the GDPR to inform the affected individual(s) of certain types of personal data breach.

If a breach is likely to result in a **high risk** to the rights and freedoms of individuals, the GDPR requires the school to inform those concerned directly and without undue delay i.e. as soon as possible.

In addition to informing the individual about the nature of the personal data breach the school must provide them with information about:

- The name and contact details of our DPO for any queries
- The likely consequences of the personal data breach
- The measures taken/to be taken to address the breach including where appropriate measures to mitigate the possible adverse effects

The school might not be required to notify the affected individual if certain exceptions apply.

3.3 Record keeping

The school will keep a record of any personal data breaches whether they are notifiable to the ICO or not including the facts of the personal data breach, its effects and the remedial action taken.

4. School's processors

Some of the school's contractors e.g. our IT suppliers process personal data on behalf of the school. The GDPR requires our contractors processing data on our behalf to notify the school without undue delay after becoming aware of a personal data breach. Our processors are required by the terms and conditions of their contracts to assist the School with any personal data breaches.

5. The School's procedures

The school has appropriate data breach procedures in place for our staff which deal with:

- reporting data protection incidents
- investigating data protection incidents
- managing data protection incidents
- containing and/or recovering data
- assessing the risk

- notification to the ICO/individual
- recording data protection incidents and action taken

6. Training:
Our staff are provided with data protection training (which includes guidance on personal data breaches) and information on how to report a data protection incident and the school's policies and procedures relating to data protection and personal data breaches.

7. Review:
This policy will be reviewed annually and updated as required.

8. Contact:
Mrs Caroline Ryan the School's Data Protection Officer c.ryan@hwjs.hants.sch.uk can be contacted with any queries about this policy.

Data breach guidance for schools

Why should we have a breach reporting process?

The GDPR requires that some, but not all data breaches must be reported to the ICO and in some cases the affected individual:

- Reporting to the ICO is required where a breach is likely to result in **a risk** to the rights and freedoms of individuals.

- Reporting a breach to the individual is required where it is likely to result in a **high risk** to their rights and freedoms.

A reportable risk exists when the breach may lead to damage to the individuals whose data have been breached. Examples of damage may include (but are not limited to) discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves Special Category Data you should assume such damage is likely.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The school will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, the school will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach

If you are not able to demonstrate that you have an appropriate process in place and that your organisation follows it, these timescales may be overlooked and, opportunities to contain the breach may be missed which could lead to enforcement action and/or a fine.

You should therefore have a written breach procedure in place. It should detail the process to follow once a breach has been detected, including how to contain, manage and recover the breach, assess the risk, and notify the breach to the ICO/individual where appropriate. You should make sure that staff are aware of the breach reporting process.

What is my role as the Data Protection Officer?

Data Protection Officers play a key role in data breach investigations, notifications on behalf of the school and record keeping. They have a duty to cooperate with the ICO and are a contact point for the ICO and data subjects.

When notifying a breach to the ICO the school must provide the name and contact details of its DPO, or other contact point.

What should my school do when there is a breach?

As soon as it becomes aware of a breach, the school must

- seek to contain the incident and
- assess the risk that could result from it.

This is important because knowing the likelihood of and the potential severity of the impact on the individual will help the school take effective steps to contain and address the breach. It will also help the school to determine whether it needs to tell the ICO and, if necessary, the individuals concerned.

For example, where personal data is accidentally sent to the wrong person in the school, or to a trusted organisation that the school has a relationship with, the recipient may be asked to either return or securely destroy the data it has received. The school might reasonably expect that the recipient in this example would not read or access the data sent in error and that they would comply with the school's instructions. This would contain the breach, reduce the likelihood of risk to individuals and may make notification to the ICO unnecessary.

How do we assess the risk?

Taking into account the specific circumstances of the breach, think about the likelihood of the individual's privacy being impacted by the breach and what that impact might be.

Your assessment should always be objective, taking into account the following criteria:-.

The type of breach
This may affect the level of risk to individuals. For example, a breach where medical information has been disclosed to unauthorised parties has different consequences to a breach where an individual's medical details have been deleted and are no longer available.

The nature, sensitivity, and volume of personal data
Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but you should also consider the context. For example, the disclosure of the name and address of an individual would not generally cause substantial damage but disclosing the name and address of an adoptive parent to a birth parent could have significant consequences for the adoptive parent and child.

Ease of identification of individuals
Consider how easy it will be for a person who has access to the personal data to identify specific individuals or match it with other information to identify individuals.

Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key.

Pseudonymisation can reduce the likelihood of individuals being identified in the event of a breach. This could be as simple as using Child A and Child B instead of names, while keeping a separate record of who it relates to.

Severity of consequences for individuals
Depending on the nature and consequences of the personal data involved in a breach (e.g. special categories of data) the potential damage to individuals could be very severe and could lead to identity theft, fraud, physical harm, psychological distress, humiliation or damage to reputation. Breaches of the personal data of children could place them at particular risk of harm.

Special characteristics of the individual
A breach may affect personal data of children or other vulnerable individuals, who may be placed at greater risk of danger as a result.

The number of affected individuals
Generally, the higher the number of individuals the greater the impact a breach can have. A breach can however have a severe impact on even one individual, depending on the nature and context of the personal data involved.

General points
Where the consequences of a breach are more severe, the risk of damage is higher. If in doubt, the school should err on the side of caution and notify the ICO and, where relevant, the individual.

How should we document the breach?

Whether you report a breach to the ICO or not, you must keep records of all data breaches –

The records should include: -

- What was the breach;
- What caused the breach;
- What personal data was affected including the categories and approx. number of records concerned;
- The categories and approximate number of data subjects concerned
- What the effects and likely consequences of the breach were;
- What remedial action was taken by the school.

You should also record the reasons for decisions taken in response to a breach, particularly, if a breach is not notified to the ICO.

If a notification to the ICO is delayed the school must be able to provide reasons for the delay and it will help if you have written evidence of this.

If you tell an affected individual about a breach you should do so in a clear, effective and timely manner and keep a record of the letter/email sent.

DATA BREACH PROCESS AND FLOWCHART

1. School receives a report of a data incident.

Schools will need to have a procedure in place for reporting data incidents to their Data Protection Officer (DPO). There is a data incident reporting form in this toolkit which your school could use.

Immediate action will need to be taken to contain the incident.

2. Has a personal data breach occurred?

The DPO will need to review the information about the incident and establish whether a personal data breach has occurred.

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 applies regardless of the format in which the personal data is held e.g. electronic, paper, image or recording.

If there are still actions which could be taken to contain the incident these will need to be undertaken immediately.

3. Assess the risk to individuals

If a personal data breach has occurred the next step is to assess the risk to the individual(s) concerned.

Is the breach <u>likely</u> to result in a risk to the individual's rights and freedoms?

If it is **likely** that there will be a risk, then schools must notify the ICO within 72 hours, if it is unlikely then schools do not have to report it.

Is the breach likely to result in a <u>high risk</u> to the individual's rights and freedoms?

If it is likely that there will be a **high risk** to the individual's rights and freedoms then the school must notify the individuals concerned without undue delay.

There could be cases where there will not be a high risk but because the individuals could learn about the breach from a third party (e.g. other parents) it would be best to notify the individual and provide them with your school's account.

NB: Please see our Data Breach Guidance for schools for more details about assessing the risk.

4. Records

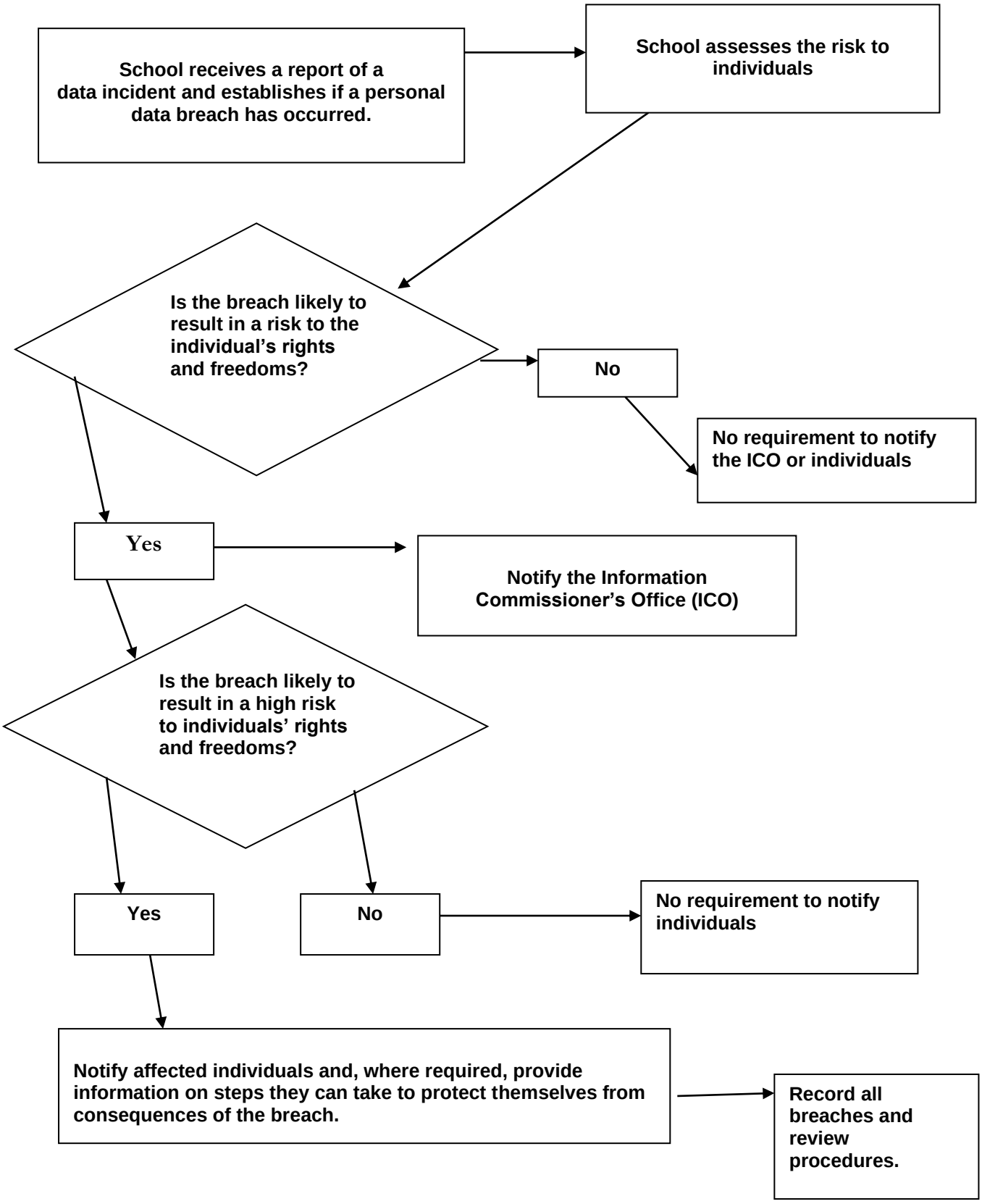
Whether or not the breach was notifiable to the ICO or the individuals a record of the breach should be made, so that you have an audit trail in case of future queries or in case the ICO asks questions about this. There is a data breach recording log in this toolkit which your school could use.

5. Review

Following a data breach, a review of your school's procedures should be undertaken to establish whether any changes are required.

If the breach was notifiable to the ICO the school's governing body should be notified of it at the next meeting. All breaches should be included in the Data Protection Officer's Annual Report (our report template can be found at: Annual Report template).

Flowchart showing notification requirements



DATA INCIDENT REPORTING FORM

The aim of this document is to ensure that, in the event of a data incident such as a personal data breach, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

This form can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who will determine the implications for the school, assess whether changes are required to existing school processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Date and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the incident. (e.g. name, addresses, health information etc.)	
How many individuals /records are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed? If so, please provide details	

IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident and the likelihood of harm to individuals?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who first became aware of the incident?	
How did they become aware of the incident?	
Form Completed by	
Position	
Date	

Data breach recording log

Details of breach						Measures taken/to be taken							
Date of breach	No of people affected	Nature of breach	Description of breach	Description of personal data	Effects and consequences of breach	Remedial action	Does the ICO need to be notified? If not explain why.	If notifiable, date of notification to ICO	If there was a delay in notifying explain reasons for the delay.	Does the data subject(s) need to be informed? If not explain why.	If data subject(s) need to be informed, date they were informed	Details of notification to any affected organisations	Notes (e.g. result of internal investigation or ICO investigation)

Other useful information

Our data breach case study and answers which can be found at:
Case study - Data Breach
Case study - Data breach - Answers

ICO guidance:

- Personal data breaches guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

- Report a breach webpage (which includes personal data breach examples to help assess the severity of a breach and a self-assessment tool to help determine whether the breach needs to be reported to the ICO): https://ico.org.uk/for-organisations/report-a-breach/

- Personal data breach reporting resources which include a webinar: :https://ico.org.uk/for-organisations/gdpr-resources/pdb/

DfE Data Protection: A toolkit for Schools which includes guidance on data breaches and a school data breach case study can be found at: https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

School Data Breach Court case:
In ST (A Minor) & Anor v L Primary School (Rev 2) [2020] EWHC 1046 a school was found to have breached the Data Protection Act by sending a letter about the behaviour of a child with Down's Syndrome to a group of parents without the child's parent's consent. A short article on the case can be found at: https://www.localgovernmentlawyer.co.uk/information-law/398-information-law-news/43711-school-breached-data-protection-and-human-rights-unlawfully-misused-personal-information-of-down-s-syndrome-pupil-and-mother-high-court

Cyber security in schools: questions for governors and trustees (July 2020):
https://www.ncsc.gov.uk/information/school-governor-questions