Wrexham County Borough Council

Data Security Incident Management Procedure for Schools

March 2022

Date Implemented:	March 2022
Review Date:	March 2025
Headteacher: Mrs Macey	
Chair of Governors: Mr Griffiths	

Document Control sheet

Title:	School Data Security Incident Management Procedure
Version:	February 2021 (Updated August 21)
Author name:	School Data Protection Officer

CONTENTS

This document is split into two parts:

Policy: Sets out the school's policy and approach to this area.

Procedure: Sets out the practical steps to be taken when incidents occur.

POLICY

1. 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.

2. School Responsibilities

2.1 Madras V.A. has a duty to comply with responsibilities under current data protection legislation to ensure that the personal data we process is kept safely and securely.

2.2 The school will manage data security incidents in accordance with the Information Commissioner's (ICO's) guidance on data breach management, which includes four essential elements:

- 2.2.1 Containment and recovery
- 2.2.2 Assessment of ongoing risk
- 2.2.3 Notification of breach
- 2.2.4 Evaluation and response.

2.3 The school will focus on minimising harm to individuals and being transparent about where mistakes have been made.

2.4 School staff will report issues of concern about data security incidents, including "near misses", in order to develop best practice, as this is seen as positive management.

2.5 A data security breach can cause undue distress and unwarranted damage to the individuals involved, disruption to school services and reputational damage to the School.

2.6 Principles within data protection legislation give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it. In order to comply with the Principles, the school must have appropriate security to prevent unauthorised or unlawful processing and to prevent accidental loss, destruction or damage, using appropriate technical or organisational measures to protect personal data.

PROCEDURE

3. Introduction

3.1 This document outlines key steps that must be taken when a data security incident, suspected breach or breach occurs.

3.2 It also provides guidance to school staff who are required to investigate a data security incident.

3.3 Where appropriate, the Schools Data Protection Officer (DPO) will report personal data breaches to the Information Commissioner within **72 hours** of the breach occurring.

4. Containment and Recovery

4.1 Once a data security incident has occurred, school staff must act immediately in order to contain the situation and minimise any damage.

4.2 All staff are responsible for reporting any incident, suspected breach or breach to the Headteacher and their School Data Protection lead, who must then report immediately to the Schools DPO.

4.3 The Schools DPO will request the School Data Protection lead, or Headteacher, carry out an initial / preliminary investigation. **This must be undertaken on the day that the incident is identified.**

4.4 Once the incident is reported to the Schools DPO, it will be allocated an Incident Number and recorded on the Schools Data Security Incident Log by the DPO.

4.5 In conducting the initial / preliminary investigation into the incident, the School Data Protection lead must complete the Schools Data Security Incident Report (Form A), which will guide the process.

4.6 The School Data Protection lead must **immediately** assess the risks and severity of the incident set out at Section 2 and 3 of Form A, and advise the Schools DPO of the score. If the score comes out as a 'Category Level 2 - score of 3 or above', the Schools DPO must decide if the matter should be reported to the ICO. This must take place **within 72 hours** of the incident occurring/being identified. The Schools DPO will also request that a Data Security Incident Investigation Report (Form B), providing additional and more detailed information, is to be completed.

4.7. The following should be established:

- 4.7.1 The date, time and location of the incident
- 4.7.2 The date the incident was discovered
- 4.7.3 The nature of incident
- 4.7.4 Details / description of the incident
- 4.7.5 Details of the immediate action undertaken.

4.8 The school should establish who needs to be made aware of the incident, so that they can assist in the containment exercise, recover any loss and limit the damage, e.g.:

- 4.8.1 Closing part of a network
- 4.8.2 Finding a piece of equipment
- 4.8.3 Changing access codes
- 4.8.4 Deciding if third parties, such as the police, need to be informed.
- 4.8.5 Advising those who are affected.

4.9 Appropriate specialist help must be engaged where necessary (e.g. School DPO, council ICT team) and the School Data Protection Lead, with appropriate support, must co-ordinate the containment and response.

5. Assessing the risks

5.1 Once the initial containment has been carried out, the next step required is to assess the risk by establishing:

- 5.1.1 The potential adverse consequences for individuals.
- 5.1.2 The potential adverse consequences for the School.
- 5.1.3 How serious or substantial the consequences are, and how likely they are to happen.

5.2 The School Data Protection lead must establish:

- 5.2.1 Details of the data involved (i.e. personal data, special category or high risk data)
- 5.2.2 The number of data subjects affected
- 5.2.3 The scale and sensitivity of the incident
- 5.2.4 The nature of data / record (paper, electronic or hybrid)
- 5.2.5 If the data was in a digital format, whether or not it was encrypted.

5.3 Important consideration must be given to the following questions in relation to the data security incident:

- 5.3.1 Could anyone have been placed in physical danger?
- 5.3.2 Could it cause emotional harm?
- 5.3.3 Could it lead to identity fraud?
- 5.3.4 Could it pose a financial risk to an individual or to the School?
- 5.3.5 Could it affect the business functions of the School?
- 5.3.6 Could it have wider implications, e.g. public health; public confidence?
- 5.3.7 Could it cause reputational damage to an individual or the School?
- 5.3.8 Are there legal implications which must be considered?
- 5.3.9 Is the incident in the public domain (e.g. published on a website)?
- 5.3.10 Is the media aware?
- 5.3.10.1 If so, the Schools DPO will notify the Marketing and Communications Team so that the Press Office can prepare for media questions.

5.4 The consequences of a data security incident will vary depending on the nature of the incident and the extent of the effect on individuals.

5.5 The more sensitive the information involved, the greater the risk of causing harm.

5.6 When the initial / preliminary investigation has been completed and the risks assessed, the School Data Protection lead and Headteacher must report to the Schools DPO to discuss what steps are necessary further to the immediate containment.

5.7 The school must keep a log of the data security incident recording all relevant information, such as dates, details of the incident, the number of individuals involved, advice received, and actions taken.

6. Assessing the Severity of the Incident

6.1 In assessing the severity of a data security incident, the School Data Protection lead must complete the appropriate section (3) in Form A - see the example of calculation in Appendix B.

6.2 There are two factors that influence the severity of a data security incident - scale and sensitivity.

6.3 In assessing the severity, this will determine the category of the incident and whether or not it is a breach and reportable to the Information Commissioner's Office (ICO).

6.4 This must be undertaken **immediately** and the Schools DPO informed, as serious breaches must be reported to the Information Commissioner's Office **within 72 hours** of the breach occurring.

6.5 **Scale Factors**

6.5.1 Although any data security incident is potentially a very serious matter, the number of individuals that could potentially suffer distress, harm or other detriment is clearly an important factor.

6.5.2 The baseline "scale" is determined by the numbers of individuals involved. This scale will be modified by a range of "sensitivity" factors.

6.6 **Sensitivity Factors**

6.6.1 Sensitivity may cover a wide range of different considerations. Each incident may have a range of characteristics, some of which may raise the categorisation of an incident, and some of which may lower it.

6.6.2 The same incident may have characteristics that do both, potentially cancelling each other out.

6.6.3 "Sensitivity" factors (as detailed in section 3.2 of the Data Security Incident Report Form A) may be:

- 6.6.3.1 **Low** – reduces the baseline scale.
- 6.6.3.2 **Medium** – has no effect on the baseline scale.
- 6.6.3.3 **High** – increases the baseline scale.

6.7 **Categorising Data Security Incidents**

6.7.1 Every incident can be categorised:

- 6.7.1.1 – a score of 2 or below is a **Category Level 1**: a confirmed data security incident, but no need to report to ICO and other central bodies.
- 6.7.1.2 – a score of 3 or above is a **Category Level 2**: a confirmed data security breach that must be considered for reporting to the ICO and other central bodies.

6.7.2 A further category of data security incident is also possible, and should be used in incident closure where it is determined that it was a "near miss" or the incident is found to have been mistakenly reported:

- 6.7.2.1 **Category Level 0:** Near miss/non-event

Where a data security incident has been found not to have occurred, or severity is reduced due to fortunate events that were not part of pre-planned controls, this should be recorded as a

"near miss" to enable 'lessons learned' activities to take place and appropriate recording of the event.

6.7.4 The Schools DPO must be notified of the score and category of the breach immediately as, if the breach needs to be reported to the ICO, this must be done **within 72 hours.**

7. Early Notification

7.1 Depending on the score of the incident, it may be managed through internal school policies.

7.2 For incidents with higher risk score, the School and Schools DPO should determine if anyone should have early notification.

7.3 If any of the following are notified (either informally or formally), details should be recorded by the School Data Protection lead on Form A:

- 7.3.1 Data subjects
- 7.3.2 Any third party organisation (e.g. the Police) Information Commissioner (ICO), Financial Services Authority (FSA)

7.4 Banks and Fraud officers may be able to advise if the loss involves financial information.

7.5 It may be necessary to notify relevant staff within the Education Department to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'. The Schools DPO should already have been made aware of the incident.

7.6 If the incident is in the public domain or in the media, the Council's Marketing and Communications Team will be advised by the Schools DPO.

7.7 Form A must be signed by both the School Data Protection lead and the Headteacher (if they are different people), and sent to the Schools DPO within 24 hours of the incident occurring.

7.8 The Schools DPO will decide if it is necessary for further investigation, or if the incident can be closed.

8. Root Cause Analysis & Investigation

8.1 If requested by the Schools DPO, the School Data Protection lead will document the investigation and findings and produce an unbiased report, using 'Form B – Data Security Incident Investigation Report'.

8.2 The School Data Protection lead will need to carry out a Root Cause Analysis of the incident.

8.3 The Incident Investigation Report will include:

- 8.3.1 Incident summary, including root cause analysis
- 8.3.2 Details of the investigation
- 8.3.3 Issues highlighted as a result of the investigation
- 8.3.4 Investigation findings and lessons learned
- 8.3.5 Actions to be taken

8.4 The School Data Protection lead must ensure that content is reviewed with sources for accuracy.

8.5 The Incident Investigation Report and Action Plan will be approved and signed by the Headteacher.

8.6 The school will forward a copy of Form B to the Schools DPO.

8.7 If deemed necessary, the Schools DPO will meet with the School Data Protection lead and Headteacher to discuss further actions

8.8 The Schools DPO will update their Data Breach incident management log, to keep a full record of the incident.

9. Notification of Breaches

9.1 Informing people about a data security breach should have a clear purpose, e.g.:

- 9.1.1 To enable them to take steps to protect themselves, e.g. cancelling credit card/changing passwords.
- 9.1.2 To allow regulatory bodies to perform their functions, provide advice and deal with complaints.

9.2 **Notifying the individuals concerned**:

9.2.1 In consultation with the appropriate specialists and the Schools DPO, the School Data Protection Lead will decide whether affected individuals should be notified, and will arrange notification.

9.2.2 Any decision not to notify those concerned must be fully documented.

9.2.3 Individuals affected by the data security breach should be provided with:

- 9.2.3.1 A description of the nature of the personal data breach, and what data was involved.
- 9.2.3.2 The contact details of the Schools DPO where more information can be obtained.
- 9.2.3.3 The likely consequences of the personal data breach.
- 9.2.3.4 Details of what has been done to respond to the risks posed by the breach.
- 9.2.3.5 Specific and clear advice on the steps they can take to protect themselves and what the school can do to help them.

9.3 **Breach Reporting**

9.3.1 When notifying the data subject(s) affected by the breach, the communication must describe in clear and plain language the nature of the breach and contain at least the information and the recommendations outlined in para 9.2.3.

9.3.2 Notifying the data subject(s) will not be required if any of the following conditions are met:

- 9.3.2.1 The School has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- 9.3.2.2 The School has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
- 9.3.2.3 It would involve disproportionate effort. In such a case, there must instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

9.3.3 The School DPO might consider consulting the ICO to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

9.3.4 Consideration also needs to be given to any prospective equality issues that may arise from a breach, e.g. the vulnerability of an individual affected by the breach.

9.4 **The Information Commissioner**

9.4.1 The decision to report the incident to the ICO will be in accordance with the guidance from the ICO.

9.4.2 Section 6 of this procedure details how the scale of the incident can be established to determine the Category Level and whether it should be reported to the ICO.

9.4.3 Section 3 of Form A must be used for this calculation.

9.4.4 Breaches that score of 3 or above (i.e. Category Level 2 breaches) must be considered for notification to the ICO.

9.4.5 The decision to notify the ICO lies with the Schools DPO.

9.4.6 The Schools DPO will be responsible for coordinating the notification to the ICO.

9.4.7 Appendix C details the actions and tools available to the ICO.

10. Evaluation and Response

10.1 An evaluation of each reportable incident will be carried out by the Schools DPO.

10.2 If the breach was caused by systemic and ongoing problems, they need to be identified and actioned.

10.3 The Headteacher or School Data Protection lead is responsible for arranging for all actions identified by the investigation to be completed.

10.4 The School DPO will monitor to ensure completion and record in the Data Security Incident Log.

APPENDIX A - Breach Types

Lost in Transit	The loss of data (usually in paper format, but may also include CDs, tapes, DVDs or portable media) whilst in transit from one business area to another location. May include data that is: • Lost by a courier; • Lost in the 'general' post (i.e. does not arrive at its intended destination); • Lost whilst on site but in situ between two separate premises / buildings or departments; • Lost whilst being hand delivered, whether that be by a member of the data controller's staff or a third party acting on their behalf Generally speaking, 'lost in transit' would not include data taken home by a member of staff for the purpose of home working or similar (please see 'lost or stolen hardware' and 'lost or stolen paperwork' for more information).
Lost or stolen hardware	The loss of data contained on fixed or portable hardware. May include: • Lost or stolen laptops; • Hard-drives; • Pen-drives; • Servers; • Cameras; • Mobile phones containing personal data; • Desk-tops / other fixed electronic equipment; • Imaging equipment containing personal data; • Tablets; • Any other portable or fixed devices containing personal data. The loss or theft could take place on or off a data controller's premises. For example the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk.

Lost or stolen paperwork	The loss of data held in paper format. Would include any paperwork lost or stolen that could be classified as personal data (i.e.: is part of a relevant filing system/accessible record). Examples would include: ▪ care plans / service delivery plans ▪ letters; ▪ rotas; ▪ employee records The loss or theft could take place on or off a data controller's premises, so for example the theft of paperwork from an employee's home or car or a loss whilst they were travelling on public transport would be included in this category. Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system).

Disclosed in Error	This category covers information which has been disclosed to the incorrect party or where it has been sent, or otherwise provided to, an individual or organisation in error. This would include situations where the information itself has not actually been accessed. Examples include: • Letters / correspondence / files sent to the incorrect individual; • Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s170 Data Protection Act 2018 (unlawful obtaining etc. of personal data) • Failure to redact personal data from documentation supplied to third parties; • Inclusion of information relating to other data subjects in error; • Emails or faxes sent to the incorrect individual or with the incorrect information attached; • Failure to blind carbon copy ('bcc') emails; • Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data; • Disclosure of data to a third party contractor / data processor who is not entitled to receive it
Uploaded to website in error	This category is distinct from 'disclosure in error' as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include: • Failures to carry out appropriate redactions; • Uploading the incorrect documentation; • The failure to remove hidden cells or pivot tables when uploading a spread-sheet; • Failure to consider / apply FOI exemptions to personal data

Loss or theft of data or equipment on which data is stored - hardware	The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include: • Failure to meet the contracting requirements of principle seven employing a third party processor to carry out the removal / destruction of data; • Failure to securely wipe data ahead of destruction; • Failure to securely destroy hardware to appropriate industry standards; • Re-sale of equipment with personal data still intact / retrievable; • The provision of hardware for recycling with the data still intact • The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of PCI compliance.
Loss or theft of data or equipment on which data is stored – paperwork	The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include: • Failure to meet the contracting requirements of principle seven when employing a third party processor to remove / destroy / recycle paper; • Failure to use confidential waste destruction facilities (including on site shredding); • Data sent to landfill / recycling intact – (this would include refuse mix ups in which personal data is placed in the general waste)
Technical security failing (including hacking)	The failure to take appropriate steps to prevent unauthorised processing and loss of data and would include: • Failure to appropriately secure systems from inappropriate / malicious access; Failure to build website / access portals to appropriate technical standards; • Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces); • Failure to implement appropriate controls for remote system access for employees (for example when working from home) In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate this risk.
Equipment/systems failure	Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects, e.g.: disruption of care, for example: • The corruption of a file which renders the data inaccessible; • The inability to recover a file as its method / format of storage is obsolete; • The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible.
Inappropriate access controls allowing unauthorised use access and disclosure	The offence under section 170 of the DPA 2018 - wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller.

Others	This category is designed to capture the small number of occasions on which a principle seven breach occurs which does not fall into the aforementioned categories. These may include: • Failure to decommission a former premises of the data controller by removing the personal data present; • The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data; • Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets). This category also covers all aspects of the remaining data protection principles as follows: • Fair processing; • Adequacy, relevance and necessity; • Accuracy; • Retaining of records; • Overseas transfers

APPENDIX B

Assessing the Severity of the Incident (Calculation Examples)

Examples:

1	Social Care data inappropriately disclosed in response to an FOI request. Data relating to 292 children, detailing their client and referral references, their ages, an indicator of their level of need, and details of each disability or impairment.		
	Baseline Scale Factor	2	
	Sensitivity Factors	-1	Limited demographic data
		0	Limited clinical information
		+1	Particularly sensitive information
		+1	Parents likely to be distressed
	Final Scale Point	**3**	**THIS IS A CATEGORY 2 REPORTABLE INCIDENT**
2	Information about a child and the circumstances of an associated child protection plan has been faxed to the wrong address.		
	Baseline Scale Factor	0	
	Sensitivity Factors	-1	No care data at risk
		0	Basic demographic data
		+1	Sensitive information
		+1	Information may cause distress
	Final Scale Point	**1**	**THIS IS A CATEGORY 1 BREACH /NOT REPORTABLE**
3	Subsequent to incident 2 (above), the same error is made again and the recipient this time informs the School she has complained to the ICO.		

	Baseline Scale Factor	0	
	Sensitivity Factors	-1	No clinical data at risk
		0	Basic demographic data
		+1	Sensitive information
		+1	Information may cause distress
		+1	Repeat incident
		+1	Complaint to ICO
	Final Scale Point	**3**	**THIS IS A CATEGORY 2 REPORTABLE INCIDENT**

APPENDIX C

Actions / Tools available to ICO:

There are a number of tools available to the Information Commissioner's Office (ICO) for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are not mutually exclusive. The ICO will use them in combination where justified by the circumstances.

The main options are:

- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- Serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Conduct consensual assessments (audits) to check organisations are complying;
- Serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice (data protection only);
- Issue monetary penalty notices, requiring organisations to pay up to €20 million for serious breaches of data protection legislation occurring on or after 25 May 2018;
- Prosecute those who commit criminal offences under data protection legislation; and
- Report to Parliament on data protection issues of concern.