

Wales Police Schools Programme
School Beat Incident Notebook

**Data Protection Compliance
Policies, Procedures and Impact Assessment**

Contents

1	Introduction to this document.....	3
2	Partner organisations.....	3
3	Data protection policy.....	4
4	Statutory basis for processing.....	5
5	Incident recording procedure.....	6
6	Retention and privacy protection.....	8
7	Impact assessment.....	10
8	Review.....	13
9	References.....	13

Status of this document

This document was published on 19/11/2021 and is effective as of that date. It may be replaced by WPSP as per section 8. The latest copy of this document can always be found at:

<https://schoolbeat.cymru/documents/wpsp-sbin>

Welsh Language / Cymraeg

This document is available in Welsh. / Mae'r ddogfen hon ar gael yn Gymraeg.

<https://schoolbeat.cymru/dogfennau/ryhc-ndsb>

1 Introduction to this document

The purpose of this document is to explain the lawful basis on which partner police forces in the Wales Police Schools Programme (WPSP) record and process data in the School Beat incident system. Procedures for ensuring compliance with the law enforcement data protection principles and policies on the retention and privacy protection of this data are detailed.

School Beat Incidents are handled as explained in the WPSP School Crime Beat Protocol ^(Reference 1). The School Beat Incident system implements a minimal level of recording to allow oversight and administration of the Protocol.

Data from the School Beat Incident system is needed to maintain a record of Police activity in relation to School Beat incidents. The process has been designed to minimise information we collect about the individual while allowing the effective administration of the justice and safeguarding work that we do.

Due to the range of incidents dealt with, some sensitive data about the health and sexual behaviour of service users may be implied. We therefore restrict access to authorised Police officers and staff.

Statistical summaries and analyses of the data are needed in order to monitor application of the Protocol, to detect and research trends in youth crime, in order that Police officers and staff can drive and direct our continuous prevention measures to safeguard children and young people.

For archiving, research and statistical purposes information is retained for the period listed in Section 6. Records which pass beyond the retention period are anonymised to protect the privacy of the individual using the procedure specified there.

Key statistics from this system are published in the annual report of WPSP.

2 Partner organisations

This document applies to all police forces which apply the WPSP School Crime Beat Protocol.

- Dyfed Powys Police
- Gwent Police
- North Wales Police
- South Wales Police

The responsible manager for implementing policy in each force is the regional lead for school liaison.

Data described in this document is jointly held and processed under the WPSP Joint Processing Agreement ^(Reference 2), for which the responsible manager and data controller is the national lead for school liaison.

3 Data protection policy

3.1 The processing of school beat incident data must at all times be lawful and fair.

We will comply with the law when handling school beat incidents. We will apply the policies and procedures in this document. We will carry out our duties in a fair manner and in accordance with our responsibilities under the Equalities Act 2010 ^(Reference 3).

3.2 Incident data must only be recorded in this system for the purposes specified in Section 4 of this document.

Processing is carried out in a proportionate way for the essential function of oversight of the School Crime Beat Protocol. Data in this system will be utilised only for the purposes specified in this document.

Current and future processing of the data must comply with Data Protection Act 2018 (DPA) ^(Reference 4).

3.3 Data recorded in this system must be adequate, relevant and not excessive.

Data recording is limited to a minimal set of characteristics which has been designed to minimise the impact on pupils spoken to. Periodic reviews will be conducted to determine if we are collecting the correct data on school beat incidents to plan and respond effectively.

3.4 Data recorded in this system must be accurate to the best of current knowledge. Any inaccuracies are to be corrected.

All officers and staff are trained in use of the system before use. Procedures for adding to incident forms and amending data are established.

Records relating to victims, witnesses, and suspects are appropriately coded. This system does not track the outcome of a criminal investigation and thus does not contain data on convictions.

Data from this system is not transferred outside the UK.

3.5 Data on this system will be managed according a retention policy which considers the needs of children. Records held long-term will be anonymised.

Retention management and anonymisation procedures are documented fully in section 6.

3.6 Data on this system will be secured to prevent unauthorised or unlawful access, modification, transfer or loss.

All data in this system is potentially sensitive to the individual. We therefore undertake to maintain a high level of protection for our data systems. Usage of the system is strictly controlled and logged, including addition, alteration, disclosure, search or transfer of records.

Where backup copies of the system are made, these will be held on police systems and destroyed within the retention timescale.

4 Statutory basis for processing

The social need answered by this system is oversight of the application of WPSA School Crime Beat Protocol, a key child safeguarding policy for Wales which describes the handling of “school beat incidents”.

Other Police systems handle the recording of crime and managing criminal investigations, in accordance with statute and force policies. School beat incidents may not result in a recorded crime or criminal investigation, and as a result the necessary oversight cannot be achieved using other systems. Within this oversight there is a requirement to understand the safeguarding issues affecting pupils in order to manage our response.

The purposes for which we process data on school beat incidents are:

- 4.1 to ensure consistent and effective safeguarding of young people through overseeing the application of WPSA School Crime Beat Protocol;
- 4.2 to safeguard young people by maintaining a log of safeguarding actions;
- 4.3 to respond to demand for incident handling;
- 4.4 to design and manage a crime prevention education programme with an aim to reduce future incidents;
- 4.5 to document, respond to and reduce harm among young people and school communities;
- 4.6 to understand the issues affecting young people who are at risk of or have encountered criminality including differences based on age group and gender.

The following DPA Schedule 8 conditions always apply:

- the data is necessary for the safeguarding of children and of individuals at risk;
- the data is necessary for archiving, research or statistical purposes.

The following condition applies when the school beat incident relates to a crime:

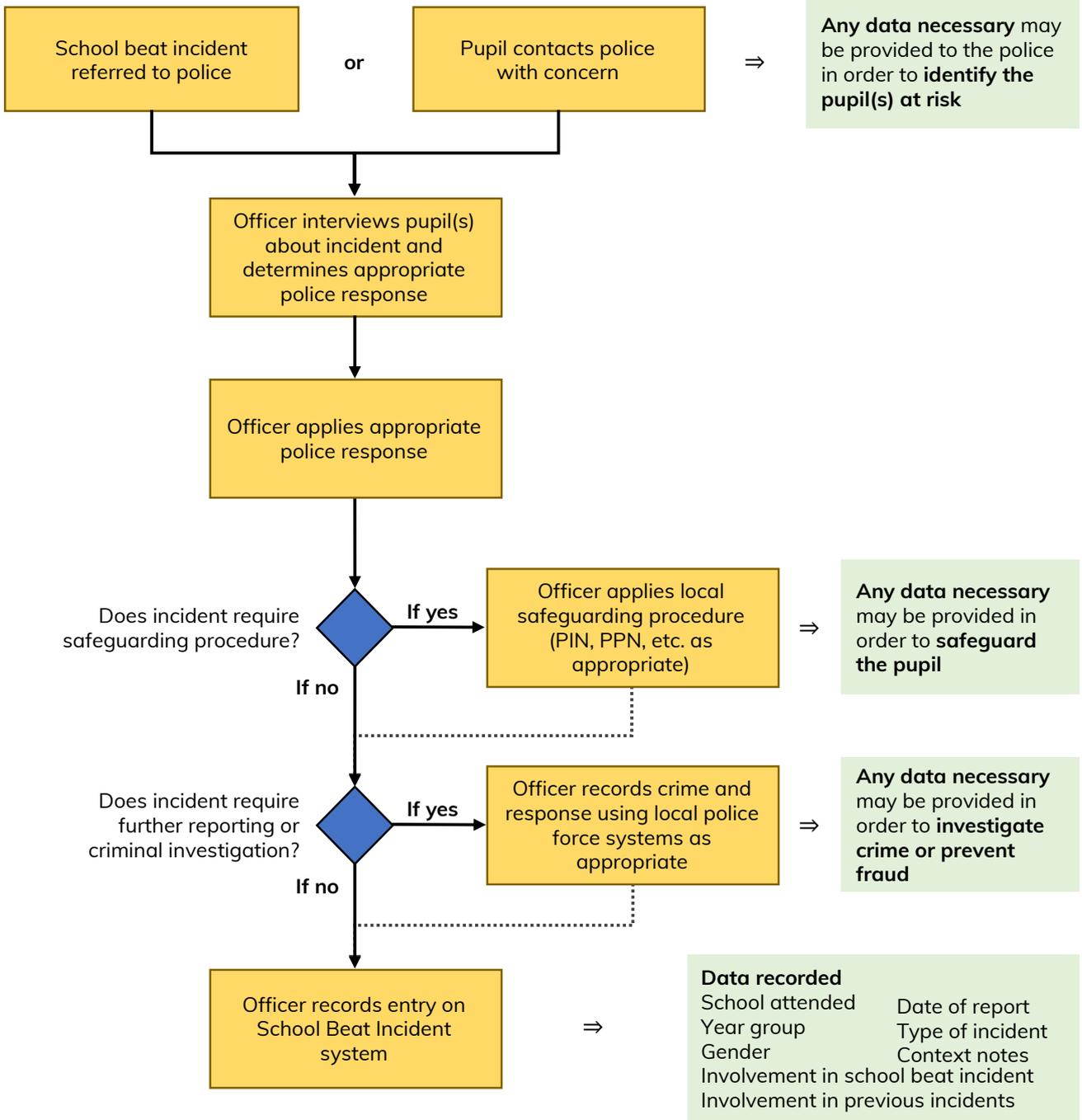
- the data is necessary for the administration of justice.

The following condition applies when the school beat incident relates to fraud:

- the data is necessary for the purpose of preventing fraud.

5 Incident recording procedure

5.1 Data Flow Diagram



5.2 Data Flow Process

Step 1: Either

A school beat incident is referred to police

or

A pupil contacts police with a concern

Police will request sufficient information to identify the child(ren) at risk. This information will be provided to the school police officer.

The minimum information needed to respond to a school beat incident is pupil name, school year, school attended, and the nature of the concern. More information (current address, date of birth) may be needed depending on the nature of the reported incident.

Step 2:

Officer interviews pupil(s) about incident and determines appropriate police response

Step 3:

Officer applies appropriate police response

Step 4: Does this incident require the officer to engage a safeguarding procedure?

If yes, the officer applies local safeguarding procedure (PIN, PPN, etc. as appropriate)

Step 5: Does this incident require further reporting or a criminal investigation?

If yes, the officer records the crime and their response using local police force systems as appropriate

Step 6:

Officer records entry on School Beat Incident system

The record will be used by WPSP to oversee application of the SCPB and for our other purposes specified in Section 4.

Any data necessary may be provided to the police in order to **identify the pupil(s) at risk.**

Any data necessary may be provided in order to **safeguard the pupil**

Any data necessary may be provided in order to **investigate crime, prevent fraud or safeguard the child**

Data recorded

Date of report
Type of incident
Context notes
School attended
Year group
Gender
Involvement in school beat incident
Involvement in previous incidents

Note: This document explains the use of data in the School Beat Incident Notebook system. The lawful basis under which data is provided to us is explained in the WPSP Information Sharing Protocol ^(Reference 5).

6 Retention and privacy protection

6.1 Rationale

We have considered how to balance young people's right to privacy and the duty to safeguard them from harm and criminality. At the time an incident is reported to the police, the record created in this system is an essential part of documenting our response to the individual and our consideration of how to best safeguard them. As time passes, the level of detail that is needed for oversight decreases. We have therefore designed procedures to anonymise school beat incident records which are only needed for archiving, research or statistical purposes.

In order to provide a usable tool for managing school beat incidents and for effective oversight, records for the current academic year and up to six previous years are kept. The rationale for this is that a period of seven academic years is typically sufficient to complete a stage of education (primary or secondary) within a school, thus marking the longest time that a record of a school beat incident would be of relevance to safeguarding children in that setting. In the case of schools which admit pupils of both primary and secondary ages, it is our assessment that the right of the child to privacy outweighs the benefit of holding the data for longer.

In the course of planning and implementing the full system described in this document, we conducted a pilot phase of recording school beat incident data. The data that we hold from the pilot has been used to assess and plan the development of the full system. Data in the pilot system is subject to all the restrictions in this document. Any statistics or summaries derived from the data are subject to the caveat that as the pilot was conducted as an opt-in trial, different time periods, areas and regions cannot be accurately compared. This shortcoming of the pilot phase decreases the benefit to the child of retaining a full record and we have opted to implement a shorter period before anonymisation to account for this.

6.2 Retention Schedule (School Beat Incident Notebook)

Meeting records are kept in their original form for up to six years from date of recording. Within six years, we will erase any notes for the incident. Within eight years, records are anonymised using procedure 6.2.1 below. Anonymised records may be retained indefinitely for statistical and research purposes.

6.2.1 Anonymisation procedure for School Beat Incident Notebook

1. Delete notes from the incident, if present.
2. Clear any identifiers from meeting records: NICHE, ORIS, SBC, UPS
3. Clear any 'See Also' records for the incident.
4. Generate a new pseudo-random incident code and change the stored incident code to this value.
5. If the school is flagged as a small school, replace the 'School attended' field with a generic value for the local authority (for example "Small Schools Blaenau Gwent").

Step 1 mitigates the risk that a record can be de-anonymised by an individual familiar with the events of the incident. Steps 2 and 3 mitigate the risk that a record could be de-anonymised by reference to other police systems or by their identifying numbers (SBC code or UPS code as originally provided). Step 4 mitigates against the risk that the incident will be de-anonymised by

an individual knowing the incident code assigned at the time of the report. Step 5 mitigates the risk that an individual can be de-anonymised based on school enrolment data.

A school is typically flagged as a small school if the pupil census of Wales identifies fewer than 30 attending pupils. Other criteria may be applied as appropriate for the school type and at the discretion of WPSP.

6.3 Retention Schedule (School Beat incident Notebook Pilot)

Meeting records are kept in their original form for up to four years. Then, they are anonymised using procedure 6.3.1 below. Anonymised records may be retained indefinitely for statistical and research purposes.

6.3.1 Anonymisation procedure for School Beat incident Notebook Pilot

1. Set the 'Ident Type' field to "none" and clear any stored identifier.
2. If the 'NICHE Occurrence' or 'ORIS Log' fields are set, replace their value with "Yes".
3. Delete all 'Incident Context' and 'Meeting Context' notes for the incident.
4. Generate a new pseudo-random incident code and change the stored incident code to this value.

Step 1 mitigates the risk that the individual met will be de-anonymised by their identifying numbers (SBC code or UPS code as originally provided). Step 2 mitigates the risk that a record could be de-anonymised by reference to other police systems. Step 3 mitigates the risk that a record can be de-anonymised by an individual familiar with the events of the incident. Step 4 mitigates against the risk that the incident will be de-anonymised by an individual knowing the incident code assigned at the time of the report.

7 Impact assessment

7.1 Risk of over- or under-criminalisation of young people

The risk that young people will be subject to more criminal investigations or greater sanctions, or that necessary investigations will not be carried out, or that individuals will face inappropriately lenient responses

Processes and mitigations against this risk

Reducing this risk is a primary purpose of this system. Monitoring and analysis of school beat incident data will be performed to address any inequalities in application of the Protocol.

This system is operated under the WSPSP School Crime Beat Protocol and does not represent a change in policy or training in relation to handling school beat incidents. WSPSP will maintain officers' understanding of the Protocol through induction training, refresher training, and information available on the SchoolBeat website.

Possibility of Harm

Remote

Potential Impact

Significant

Overall Risk

Medium

7.2 Risk of over- or under-provision of school police officers

The risk that the presence or absence of school beat incident records will lead to an excessive or insufficient level of policing being provided to a school.

Processes and mitigations against this risk

Regional coordinators for school liaison are responsible to assigning school police officers' areas of responsibility. This process is based on human decision-making; statistics and reports from this system will inform the regional coordinators but will not be used to automate the decisions made.

The school police officer role involves delivering a programme of lessons as well as dealing with school beat incidents; as such each participating school is assigned to an officer post regardless of the number of incidents at a school.

In the event that a school beat incident or incidents should require the attention of more than one officer, additional support will be assigned. This support would be needed before incident records exist and thus this system could not generate or cause such requests for additional police support; the assignment of school beat incidents shall remain the responsibility of officers and their management.

Possibility of Harm

Remote

Potential Impact

Minimal

Overall Risk

Low

7.3 Risk of identification

The risk that an individual can be associated with a school beat incident based on data in the incident record or data from other systems, and that this identification leads to a change in how they are treated

Processes and mitigations against this risk

It is necessary for police personnel to identify individuals spoken to in relation to previous incidents, in order to understand the context of a later incident. To protect the individual's privacy, we record the minimum information needed to identify them, and restrict access to authorised personnel.

Following anonymisation of the record, this risk is minimised.

Possibility of Harm
Possible

Potential Impact
Minimal

Overall Risk
Low

7.4 Risk of inappropriate identification

The risk that an individual can be associated with a school beat incident through processes other than allowed in this document

Processes and mitigations against this risk

We restrict access to authorised personnel and will not engage in data transfers which would enable the identification of individuals in other contexts.

Possibility of Harm
Remote

Potential Impact
Minimal

Overall Risk
Low

7.5 Risk to an individual's right to be forgotten

The risk that information will continue to affect an individual's treatment for an excessive amount of time

Processes and mitigations against this risk

Retention and anonymisation periods for our data have been set to match a single phase of schooling (primary / secondary). Beyond this time frame, records are anonymised and are no longer individually identifiable.

Possibility of Harm
Remote

Potential Impact
Minimal

Overall Risk
Low

7.6 Risk of future bias

The risk that the recording of an individual's involvement in a school beat incident will prejudice the investigation of future incidents

Processes and mitigations against this risk

Accurate recording of school beat incidents in this system should improve the consistency of handling across Wales and thus reduce the opportunity for individual bias. Further, officers are trained in the avoidance of bias, including bias based on prior incidents.

Possibility of Harm
Possible

Potential Impact
Moderate

Overall
Medium

7.7 Risk of improper access

The risk that records of school beat incidents will be accessed for an improper purpose, or that they will be accidentally destroyed or published.

Processes and mitigations against this risk

Data in this system will be accessed for a policing purpose as specified in this document. Technical security restrictions will be put in place such that only authorised personnel may access the system. Personnel will only be able to access data relevant to their assigned area of operation.

Backups of this data will be held on Police systems only and erased within the retention schedule.

All activities on this system will be logged and any improper access detected will be investigated. Any breach of our systems will be reported to the UK Information Commissioner's Office.

Possibility of Harm
Remote

Potential Impact
Significant

Overall Risk
Medium

7.8 Risk of child criminal exploitation

The risk that data in the system could be used by those with criminal intent to identify children vulnerable to exploitation.

Processes and mitigations against this risk

Mitigations to protect the individual's privacy apply to this risk, as such targeting would first involve identifying the individual. These are described above in 7.3, 7.4 and 7.5.

We secure our data from improper access, as described in 7.7.

Possibility of Harm
Remote

Potential Impact
Severe

Overall Risk
Medium

8 Review

This document will be reviewed every two years to ensure that our policies and procedures are adequate for the task of safeguarding children. The manager responsible for leading the review is the national lead for school liaison.

Later versions will replace this document and come into force when they are issued. The SchoolBeat.cymru website will be used to publish revisions to this document.

9 References

¹ Wales Police Schools Programme: School Crime Beat Protocol
<https://schoolbeat.cymru/documents/wpsp-scbp>

² Wales Police Schools Programme: Joint Processing Agreement
<https://schoolbeat.cymru/documents/wpsp-jpa>

³ UK Government: Equalities Act 2010
<https://www.legislation.gov.uk/ukpga/2010/15/contents>

⁴ UK Government: Data Protection Act 2018
<https://www.legislation.gov.uk/ukpga/2018/12/contents>

⁵ Wales Police Schools Programme: Information Sharing Protocol
<https://schoolbeat.cymru/documents/wpsp-isp>