Information Security Breach Procedure

Author	Data Protection Officer
Review Cycle	Biennially
Date Approved	February 2024
Approved By	Board of Directors
Next Review Date	February 2026

1. Introduction

1.1 This procedure supports the School's Information Security Policy (SISP) and **must be read in conjunction** with it. This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII – see 1.2 for examples) by school employees, Governors or third parties[1] contracted to provide school services.

1.2 Some typical examples of PII include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Special Category (sensitive) Personal Data –** e.g. information specifically relating to race and ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, biometric data identifying individuals, genetic data, health data, sexual preferences, sex life and/or sexual orientation

1.3 The principles of securing information (in accordance with Principle 6 of the UK Data Protection Act/UK GDPR 2018), can be found in the Schools Information Security Policy (SISP). For further guidance on information security contact the Data Protection Officer (DPO).

2. What is a possible breach of PII?

2.1 A breach of PII is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Article 4(12) – GDPR). A breach is where personal data has been viewed in an unauthorised way by a 'non-trusted' third party.

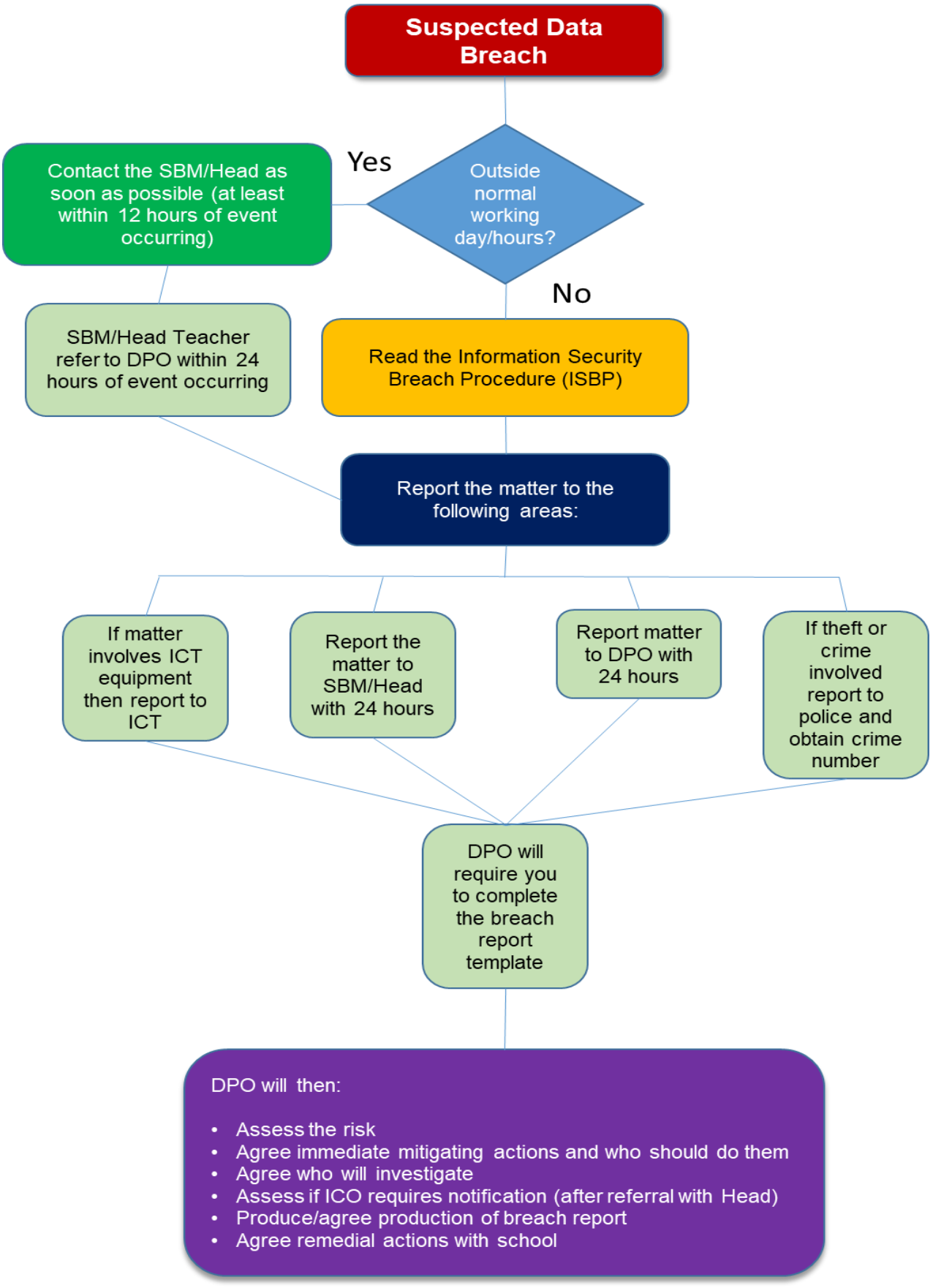
There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
- PII being emailed/posted/ to an unintended recipient or address and read by the individual, e.g. a letter containing child protection information or financial information about an individual being sent to 36 Smith Street instead of 63 Smith Street (the intended recipient) and opened
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personnel information
- Viewing PII that you do not need to access as part of your role
- Not keeping personal information secure; i.e. leaving correspondence on your desk at the end of the working day

2.2 An incident is where personal data has been sent and viewed by a 'trusted' third party, e.g. the police, health, etc or sent to a 'non-trusted' third party and not read. There may be security incidents where PII has been given to an unauthorised person (due to a human or procedural error) but the recipient has not opened/read the PII. The PII has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be notified to the DPO and the school will be expected to undertake their own investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future. Breaches and incidents are treated in the same way in terms of investigating and reporting but an incident would be much lower risk than a breach so would not need to be reported to the ICO.

[1] Third parties could include temporary employees, agency workers, volunteers, partners or contracted service providers

3. What should I do if I become aware of a possible data breach?



3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact the School Business Manager (SBM)/Head Teacher within 24 hours of the incident occurring and then follow 3.2 below.

3.2 Normal working day

3.2.1 If you know/suspect a breach has occurred you will need to inform the SBM or Head Teacher immediately (or as a minimum within 24 hours of incident occurring). The matter must then be forwarded to the DPO within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then you should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the IDT Service Desk / ICT Technician.

3.2.4 When the matter is reported to the DPO and IDT (where relevant) the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- School employee or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted if applicable
- Confirmation as to who else in the school has been informed, e.g. SBM, Head Teacher, etc.

3.2.5 When the incident is reported to the DPO they will:

- Assess the level of the risk associated with the incident
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the breach
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the Head) if applicable
- Agree the production of a breach report, see ***Appendix 1*** for required layout
- Agree remedial action to be taken
- Communicate any lessons learnt school-wide where appropriate

3.2.6 Managers can obtain guidance on possible action to be taken in relation to employees implicated in data breaches by discussing with Human Resources.

2. 4. Advice and assistance

4.1 If you require any further information please contact the SBM or DPO (email IG@telford.gov.uk).

Appendix 1

Suggested Report Template

(Input in grey below are example entries only)

Tick relevant box

Breach?	✓	Incident?	

See section 2 of this procedure for guidance on what constitutes a breach or incident

Date Occurred	12/12/23	Officer Causing the Breach	R Montgomery

Date and name of SBM informed (and Head where relevant)	Was breach/incident identified as a result of a complaint (Y or N?)	
13/12/12/23 – Anthea Lowe		*Y*

Categories of Data Breached	Number of Individuals Affected	Number of Records Breached
Name, Address, Bank details	*1*	*6*

Description of breach/incident (including the type of information and date/location of incident)

Bank statements collected for identification purposes returned to 15 Darby Road on 11/12/23 instead of correct address 51 Darby Road

Reported to police Y/N?	*N*	Date Reported / Police Station	*N/A*	Crime number	*N/A*

Has information been returned to School or destroyed?	Do you intend to notify the data subject(s) affected? If YES please consult DPO prior to doing this If NO please give an explanation for this
Information returned to School on 11/12/23	*Yes – as they will be able to ask their bank to watch their account*

How did breach/incident occur?

Employee had incorrectly updated the contact record for this parent

Measures already taken to address breach

1. Procedures for updating contact records reissued to all staff
2. Warning of this incident emailed to all staff
3. QA checks to be put in place monitoring contact records accuracy

Description of action (if any) taken against officer implicated in the breach/incident

Informal discussion with Head and warning about future conduct

Lessons learnt to be implemented (if relevant)

1. Procedures for updating contact records reissued to all staff
2. Warning of this incident emailed to all staff
3. QA checks to be put in place monitoring contact records accuracy