Data Breach Notification Procedure

TABLE OF CONTENTS

PROCEDURE OVERVIEW.

This document provides guidance to Wiltshire Police and Office of Police and Crime Commissioner (OPCC) employees on their responsibilities when becoming aware of a personal data breach, and the subsequent decision making process for notifying the Information Commissioner's Office (ICO)*.

All staff are to familiarise themselves with this procedural document. It is vital that a potential data breach is notified to either the Force Data Protection Officer or the Assistant Data Protection Officer at the earliest opportunity, using the Data Breach Notification Form (Appendix A), to ensure any onward referral to the ICO is made within 72 hours of the incident.

If a loss, theft, unauthorised disclosure or compromise of non-personal data occurs then it will not be necessary to consider whether or not to notify the ICO.

GLOSSARY OF TERMS.

Term	Meaning
DP	Data Protection
DPA	Data Protection Act
UKGDPR	UK General Data Protection Regulation
ICO	Information Commissioner's Office
SIRO	Senior Information Risk Officer

PROCEDURE.

1. Legal Requirements.

The processing of personal data is governed by the UK General Data Protection Regulation (UKGDPR) and Data Protection Act (DPA) 2018. Under this legislation all data controllers (the Chief Constable in the case of Wiltshire Police, PCC in the case of the OPCC) have a responsibility to ensure appropriate and proportionate security of the personal data that they process. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

When a data controller becomes aware of a personal data breach for which the controller is responsible, the controller has a legal obligation to notify the breach to the Information Commissionaire Office (ICO) without undue delay and where feasible, not later than 72 hours after becoming aware of it. Where the notification is not made within 72 hours, the notification must be accompanied by reasons for the delay.

If the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals there is no requirement to notify the ICO. However, such a decision must be fully documented by the DP Leads.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controlled shall communicate the personal data breach to the data subject without undue delay.

2. What is a Personal Data Breach?

A 'personal data breach' means an incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

3. What should you do when you become aware of a Personal Data Breach?

In the event that you become aware of personal data breach you must notify the Data Protection Officer as soon as is practicable, by completing the Data Breach Notification Form and emailing it to the DPO Inbox: DataProtectionOfficer@Wiltshire.police.uk

If the breach is likely to result in a high risk to the subject(s) of the personal data breach, it may be necessary to contact the Data Protection Officer or Assistant Data Protection Officer immediately by phone or email, and follow up with the completion of this form.

Remember that the Controller is required to inform the Commissioner without undue delay and within 72 hours of becoming aware of a personal data breach unless it is unlikely to result in a **risk** to the rights and freedoms of an individual or individuals.

Should you become aware of a Personal Data Breach where the period of non-working hours would exceed the stipulated 72 hours, e.g. a long bank holiday weekend, please contact the Data Protection Officer or Assistant Data Protection Officer for further advice.

****If a loss, theft, unauthorised disclosure or compromise of non-personal data occurs then it will not be necessary to notify the ICO.****

4. Notification to the ICO.

The Data Protection Officer will make an assessment of the personal data breach and determine whether the breach will be notified to the ICO. As previously stated, if reporting the breach, this must be done within 72 hours of it coming to notice.

Ordinarily notification should occur **as soon** as the information required in the Data Breach Notification Form is available. However; consideration must be given as to whether notifying the ICO could prejudice an ongoing investigation or operation and if so it may need to be delayed.

If the report is not made within 72 hours, when it is subsequently provided it must be accompanied by an explanation of the reasons for the delay.

The Notification Matrix (Appendix B) will help to determine whether a loss, theft, unauthorised disclosure or compromise of personal data is 'significant' and therefore should be reported to the ICO. Fundamental to this matrix is the use of the National Decision Model and that normal force policies such as Critical Incident investigation are not superseded by it, but that factors are considered in light of it.

The use of individual discretion is not prevented. Acting outside of this guidance is permitted where the decision can be justified and the rationale is recorded in sufficient detail. Examples of circumstances where the use of discretion may be considered are where the loss is a repeated incident or where there is significant impact on public confidence. Adherence to the National Decision Model (underpinned by the Code of Ethics) and Competency Values Framework may facilitate making discretionary decisions of the highest professional standards of public service.

Whilst the model below is purely referring to the data subject and ICO notification, it is expected to operate within, and therefore also be assessed within, the operational context of any related or directly connected incident. This will ensure that the primary concern of public safety is always paramount.

Where the breach is a critical incident and a Gold Group has formed, the timing of ICO notification will be a matter for their consideration and discussed with the SIRO. Where the matter is not a critical incident, the Data Protection Officer will liaise with the senior manager of the relevant business area to establish whether a delay is required and will inform the SIRO. The Data Protection Officer will also make the Head of Corporate Communications aware of any subsequent decision to notify the ICO. This is necessary to manage any media 'fall out'.

If it is determined that the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals there is no requirement to notify the ICO. The rationale and outcome of notification decisions should be recorded by Data Protection Officer as part of the incident record within the appropriate 'Data Breach folder'.

Notification to the ICO will be made to the ICO Breach Specialist Team by: **Email** - **icocasework@ico.org.uk**.

5. Notification to the Data Subject.

Where a personal data breach is likely to result in a **high risk** to the rights and freedoms of individuals, you must inform those individuals directly and without undue delay. The threshold for communicating to individuals is higher than for notifying the Information Commissioner. A data protection impact assessment made prior to the breach may provide an initial assessment of such risk.

When considering whether such a breach seriously interferes with the rights and freedoms of an individual or individuals, remember that this could include emotional distress and physical and material or non-material damage. It would not for example mean possible inconvenience; each must be considered on a case by case basis taking account of all the relevant factors. Think about the likelihood of anything occurring as a result of the breach and the likely impact.

There will be circumstances when it will not be necessary to inform the data subject, for example:

1. where appropriate technological and organisational measures have been put in place prior to the breach e.g. adequate encryption or
2. where subsequent immediate steps have been taken to ensure the high risk to the rights and freedoms of the individuals is no longer likely to materialise, N.B. due regard must still be given to the confidentiality of the personal data, or
3. it would involve disproportionate effort. However, the information must still be conveyed in another form e.g. via a public forum such as a website.
4. where the personal data comes Law Enforcement Processing, the provision of the information to the data subject can be restricted, wholly or partly, provided there is regard to the fundamental rights and legitimate interests of the data subject and it is a necessary and proportionate measure to:
    - avoid obstructing an official or legal inquiry, investigation or procedure;
    - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
    - protect public security or national security or protect the rights and freedoms of others.

Where communication to the individual is deemed to be necessary, and taking account of any Law Enforcement considerations (as stated above at point d), it should be made as soon as possible. This will allow an individual to take any necessary steps to protect themselves, their personal data and/or their assets.

Notification to the Data Subject(s), and without undue delay, must include:

1. a description of the nature of the breach;
2. the name and contact details of the Data Protection Officer or someone who could provide more information about the breach;
3. the likely consequences of the breach;
4. the measures taken, or those proposed to be taken, to deal with the personal data breach, including any measures taken to mitigate any possible adverse effects;
5. this information must be conveyed in a clear, concise and easily understood language and in an accessible form.

Where the decision is taken not to inform the data subject(s) of the breach the Commissioner may still require the Controller to do so at a later stage.

N.B. There may be other requirements to notify under other associated legislation or your insurers or the IOPC (liaise with the Professional Standards Department and/or Legal Department).

6. ICO Action.

The nature of the breach or loss will be considered by the ICO together with whether the Force is properly meeting their responsibilities under current legislation. The ICO will also advise the Force, if asked, on how to manage and minimise the impact of the loss on the data subject. The ICO will make an assessment of the personal data breach and determine whether the Force will be subject to any enforcement action.

Any individual who becomes aware of the loss of their own or someone else's personal data can make a complaint directly to the Information Commissioner. Any such complaint will normally trigger an investigation by the ICO. Whether or not the incident had already been

reported by the organisation involved would normally be considered by the investigators and the subsequent judgement. 'Serious' breaches are not defined by the ICO.

RELATED DOCUMENTS and Authorised Professional Practice.

Data Protection Policy
Information Security Policy
NPCC Data Protection Manual of Guidance

DATA PROTECTION AND FREEDOM OF INFORMATION.

This procedure is compliant with the obligations placed on Wiltshire Police in accordance with the UK General Data Protection Regulation (UKGDPR) and Data Protection Act (DPA) 2018.

This document has been assessed as suitable for public release.

HUMAN RIGHTS AND EQUALITY IMPACT.

This procedure has been drafted to comply with the principles of the Human Rights Act 1998 and Equality Act 2010. Members of Wiltshire Police administering this procedure are responsible for ensuring that in its application, those to whom the procedure applies, shall not receive less favourable treatment because of their age, colour, disability, ethnic or national origin, gender re-assignment, marital status, nationality, race, religion, sex or sexual orientation.

This policy has been subject to an equality impact assessment and has been graded Low Impact.

(This form is also available on the Forms and Templates page)

Appendix A: Data Breach Notification Form.

Wiltshire Police – Data Breach Reporting Form

Introduction
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

All personal data breaches must be reported to the Information Commissioner's Office (ICO) where feasible not later than 72 hours after becoming aware of the breach. Therefore, in the event that you become aware of personal data breach you must notify the Data Protection Officer as soon as is practicable, by completing the below form and emailing it to them.

If the breach is likely to result in a high risk to the subject(s) of the personal data breach, it may be necessary to contact the Data Protection Officer immediately by phone or email, and follow up with the completion of this form.

The Data Protection Officer will make an assessment of the breach, and determine whether the breach will be notified to the ICO.

Please provide the details of the data security breach by completing the below:

1. Contact Details	
Name of person reporting the incident / Incident Lead (name and shoulder number):	
Contact Details (Telephone and email address)	
If applicable, name of person(s) responsible for the breach	
2.Summary of the Security Incident	
Date and time of the breach:	
Date and time the breach was discovered (if different to the above):	
Nature of the breach (e.g. Theft, loss, disclosed in error, technical problem etc)	
How did you become aware of the breach?	
Description of the data breach - Please describe the incident in as much detail as possible, outlining the circumstances to include a description of the data breached i.e. crime file, disc etc:	
3. Reporting	
Incidents should be reported to the ICO within 72 hours - If there has been a delay in reporting the incident internally, please explain your reasons for this:	
Who have you / who is informed of the data breach (i.e. supervisor)?	
4. Personal Details	
Provide the details of the personal data that has been placed at risk?	
How many individuals are affected by the breach?	
Number of personal data records concerned?	
Are you aware whether the information breached has been further shared? If so, please provide details.	
Was the data protected? E.g. Encrypted?	
What could the breach tell a third party about the individual's involved?	

Are the affected individuals aware that the incident has occurred? If so, how was this communicated?	
What are the potential consequences and adverse effects on those individuals?	
What is the likelihood that data subjects will experience significant consequences as a result of the breach?	
5. Data Retrieval	
Have you taken any action to minimise/mitigate the effect on the affected individuals?	
Has any containment / counter compromise action taken place to limit impact of this breach?	
Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred:	
If not already recovered, what action can be taken to recover the data?	
6. Organisational measures	
Have staff involved in this incident completed their mandatory Data Protection Training? If yes, provide the date completed.	
Have there been any formal communications around the data breach?	
Have any affected individuals complained to the organisation about the incident?	

Complete this form, save it and email it to: DataProtectionOfficer@wiltshire.police.uk

If you would like to speak to someone about the incident / breach or about completing this form please contact the Force Data Protection Officer.

Appendix B: Notification Matrix (ICO and Data Subject).

Low likelihood of detrimental impact to the data subjects' rights and freedoms	Medium likelihood of detrimental impact to the data subjects' rights and freedoms	High likelihood of detrimental impact to the data subjects' rights and freedoms
N.B. These are not specific examples, they are a guide only and each must be considered on a case by case basis, e.g. trusted recipients – in most cases disclosure to a trusted partner will be unlikely to result in a risk but this won't always be the case.	**N.B. These are not specific examples, they are a guide only and each must be considered on a case by case basis, e.g. significant volumes of personal data have been disclosed – volume isn't necessarily relevant. Even one piece of sensitive information could be enough to require notification to**	**N.B. These are not specific examples, they are a guide only and each must be considered on a case by case basis. Where the personal data comes under Part 3, the provision of the information to the data subject can be restricted, wholly or partly (further details can be found in this document).** • Data is in the public domain/very likely to be placed in the public domain

• Data already in the public domain by other means or very unlikely to be published • Trusted recipients e.g. statutory partners and/or unlikely to have intent to harm or publish and/or advised about confidentiality • Access to data unlikely/deemed very difficult due to security measures, e.g. encryption • Data fully recovered with no exposure/no further exposure • Data is not defined within Special Categories* • Data can be restored/recovered in a timely manner with little impact • Extremely difficult to match personal data to a particular individual	**the ICO. Similarly, loss of lots of information that is unlikely to result in a risk will not need to be reported.** **E.g. the data is unencrypted – it depends on the nature of that held on the unencrypted device - what is the risk to individuals of this information potentially being accessed by unauthorised third parties?** • Data likely to be placed in the public domain • Individual(s) may suffer embarrassment or distress • Data is not Special Category* data • Individual is potentially vulnerable • Identification could be possible but data recipients unlikely to have either intent or skills to do so	• Individual(s) is/are likely to suffer embarrassment/distress/reputational damage/discrimination • Individual(s) may become victim(s) of crime / recipients have malicious intent • Individual(s) may suffer identity theft/financial loss • Significant volumes of personal data have been lost, disclosed or compromised • Special category data* • Easy to identify specific individuals/match data with other information to identify individuals. • Individual is vulnerable
Low likelihood of detrimental impact to the data subjects' rights and freedoms	**Medium likelihood of detrimental impact to the data subjects' rights and freedoms**	**High likelihood of detrimental impact to the data subjects' rights and freedoms**
• No risk to the rights and freedoms of affected individual(s) • Impact is inconvenience and/or annoyance Amount of data is low and provides no significant impact on individual(s)	• Significant volumes of personal data have been lost, disclosed or compromised • Risk to the rights and freedoms of individuals • The data is unencrypted • Loss of confidentiality and/or availability and/or integrity of the personal data Measures taken in a timely manner, to reduce the impact on the rights and freedoms of an individual(s)	• Individual(s)' rights cannot be met due to personal data availability issues • Disproportionate efforts (other means to be used)
ICO **does not** need to be notified	Data loss **must** be reported to the ICO	Data loss **must** be reported to the ICO. Data subject **must** be informed of the data loss.

Data subject **does not** need to be informed of the data loss *NB Keep under review in case circumstances change*	No legal requirement to notify data subject; consider any ethical/policy/operational or other reasons for doing so. N.B. Consider Part 3 obstructing/prejudicing aspects and consulting with OIC/specialist dept. – see 2d(iv)	N.B. Consider the Part 3 obstructing/prejudicing aspects and consulting with OIC/specialist dept. – see 2d(iv)

*Special Categories of personal data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex or sexual orientation.

** This table is a guide only; each breach must be considered on a case by case basis.

Revision History

Version	Date	Summary of changes
2.0	25.08.2024	Reference and applicability to the OPCC added and made clearer.
2.0	15.04.2024	Review and update.
2.0	26.04.2024	v2.0 adapted onto new SharePoint procedure template