POLICE & CRIME COMMISSIONER

Serving Hampshire
Isle of Wight
Portsmouth
Southampton

Data Breach Policy and Procedure

Author:	*Acting Head of Governance and Policy*
Date created:	*May 2018*
Review due/frequency:	*Annual*
Version:	*1.2 Published*
Current Version Date:	*September 2018*

1. Introduction to the Data Breach Policy and Procedure

1.1 As a data controller, the Police and Crime Commissioner (PCC) is aware of its responsibilities under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) to ensure appropriate and proportionate security of the personal data we hold.

1.2 The PCC has a duty under the principles of the GDPR to ensure that the personal data it stores and uses is kept safe and secure, and protected from loss, destruction or unauthorised disclosure.

1.3 The PCC has a duty under the GDPR to report certain types of personal data breach to the Information Commissioner's Office.

1.4 Although technical and organisational measures are taken to prevent the unauthorised or unlawful processing of personal data, there may be occasions when this happens.

1.5 This policy and procedure outlines the position of the organisation in respect of such incidents, and the action that needs to take place as a consequence.

1.6 This policy applies to all staff within the Office of the Police and Crime Commissioner, to agency, associated and affiliated workers, and to its volunteers.

1.7 This policy should be read in conjunction with the PCC's Data Protection Policy.

2. What is personal data

2.1 Personal data consists of personal data, special category data (previously known as sensitive data) or criminal offences data which can be linked to and/or identifies services users or employees. The PCC's Data Protection Policy contains further information.

3. Definition of a data breach:

3.1 A 'personal data breach' is defined in the GDPR as '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'. 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.

3.2 Data breaches can happen for a number of reasons. They include:-
- Loss or theft of data of equipment on which data is stored;
- Inadequate access controls allowing unauthorised use;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- alteration of personal data without permission;
- loss of availability of personal data;
- unforeseen circumstances such as a fire or flood;
- hacking attack.

3. Responsibility of staff

3.1 It is the responsibility of all staff members, contractors and volunteers to be aware of what constitutes a data breach, and the action that needs to be taken in the event of a breach.

3.2 All staff members, contractors and volunteers will be provided with training to be made aware of their responsibilities, through a combination of e-learning, face-to-face information sessions and regular updates from the Data Protection Officer.

3.3 Following any data breach, the primary responsibility of the organisation is to contain the breach, which will often involve input from specialists across the business such as communications, HR and IT. Successfully doing this requires the right people being notified in a timely manner, and those staff prioritising the response to any breach above other pieces of work.

3.4 The staff charter of the organisation encourages staff to behave with honesty and integrity. In the context of data breaches, this means that any breaches should be reported to their manager as soon as possible. Staff members should not attempt to 'cover up' or recover the breach without informing their manager because of a fear of disciplinary action. If the breach has been the result of a genuine mistake rather than deliberate misconduct, the organisation will work with individuals to learn from it and put measures in place to minimise the risk of it occurring in the future

4. Immediate steps staff should take

4.1 If there is a data breach staff should:

- Immediately notify their line manager;
- Take steps to retrieve the personal data;
- Notify the Data Protection Officer as soon as possible. In the absence of the DPO, staff should contact another senior manager and they will if necessary contact the Joint Information Management Unit (JIMU) of Hampshire Constabulary/Thames Valley Police for supporting in implementing this procedure;
- Complete the data breach notification form as soon as possible.

The DPO will then implement the procedure for assessing and managing the incident as outlined further in this document.

5. Breach management

5.1 The PCC will implement a four step plan: containment and recovery; assessment of ongoing risk; notification of breach; and evaluation and response. Further guidance on this is available in appendix A, drawing upon advice from the ICO.

Step 1: Containment and recovery

Once the DPO has been notified of the personal data breach the DPO will do the following as required in the circumstances:

- Take any immediate steps to prevent any further breach of the same data. ie. suspending processing activity;
- Notify the Chief Executive and PCC as appropriate;
- Notify the Head of Communications and Engagement;
- Appoint a senior manager to investigate the breach (usually this will be the senior manager for the relevant business area);
- Convene a proportionate breach response team to carry out actions;
- Consider representation where relevant from communications, HR and IT;
- Consider informing the JIMU if relevant;
- Notify any other affected organisations.

Step 2: Assessment of ongoing risk

The senior manager will carry out an initial assessment of the risk and then meet with the DPO to agree the risk level.

The senior manager will assess the incident by conducting a risk analysis using a likelihood vs impact assessment. The senior manager should take into account following considerations, together with any other relevant factual information in order to determine whether an incident is a 'near miss', 'minor' or 'serious':

- **The type of breach -** this may affect the level of risk to individuals.
- **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 context should always be considered.
- **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.
- **Severity of consequences for individuals -** depending on the nature and consequences of the personal data involved in a breach (e.g. special category 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.
- **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 only one individual depending on the nature and context of the personal data involved.

- **General points** – when assessing the risk that is likely to result from a breach, consideration should be given to a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Where the consequences of a breach are more severe, the risk of damage is higher and similarly where the likelihood of these occurring is greater, the risk of damage is also heightened. If in doubt, the organisation will err on the side of caution and notify the ICO.

Step 3: Notification of breach

The PCC has a duty under the GDPR to report a personal data breach that is likely to result in a risk to the rights and freedoms of individuals to the ICO within 72 hours.

The assessment of the risk will identify if the breach meets the threshold for notification.

The DPO will report any notifiable breaches to the ICO by one of the following methods:

- By telephone on 0303 123 1113 (M-F 9.00am - 4.30pm).The ICO can give advice about what to do next including whether you need to tell the data subjects involved.
- Using the ICO's online form:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO shall contact the individual concerned about the breach without undue delay and in any event within 5 working days.

The DPO will complete an entry in the personal data breach register.

The DPO will notify other affected organisations not already notified if relevant.

A communications strategy will be prepared if a decision is made to report to either the ICO, the data subject or both.

Step 4: Evaluation and response

The DPO, senior manager and breach response team will review actions of the organisation and propose changes to policies and procedures. Any advice or requirements from the ICO will be acted on.

Consideration will be given to any additional training requirements for staff.

Consideration will be given to any technical solutions which could prevent a repeat of the breach.

A debrief meeting with affected staff will be held to ensure it is a learning experience.

5. Our organisation as a data processor

5.1 Where the OPCC is a data processor, an agreement will be in place that governs the process for reporting any data breaches to the data controller.

5.2 The contract manager should make themselves aware of the provisions within any agreement that dictates how and in what timescale any data breach should be reported to the data controller for the information affected.

5.3 In any event, under the GDPR a processor must notify the controller 'without undue delay' after becoming aware of a personal data breach. Where the PCC is a processor it should provide information to the controller promptly to enable them to comply with their duty to report certain types of personal data breach to the ICO within 72 hours. The PCC may have to provide information to the controller in phases in order to meet its statutory obligations and any contractual obligations.

6. Breach register

6.1 The PCC is required to document any personal data breaches comprising the facts relating to the personal data breach, its effects and the remedial action taken. This information will be recorded in a breach register which will enable the ICO to verify compliance with the GDPR.

7. Sources of further information

7.1 Guidance can be sought in the event of a breach from the following sources:

- Article 29 Data Protection Working Party **Guidelines on Personal data breach** notification under Regulation 2016/679;
- ICO Guidance on data security breach management*
- ICO Guidance on notification of data security breaches*

*Please note these guides are pre GDPR and DPA 2018 and must be read with caution.

Data Breach Policy and Procedure – Appendix A

Phase	Relevant sections of ICO Guidance	Actions for OPCC to consider
1) Containment and recovery	Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following: Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door. Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.	Notify the Data Protection Officer, who will in turn inform the Chief Executive (and PCC as appropriate). Notify the Head of Communications and Engagement. Appoint a senior manager to investigate the breach. This is likely to be the senior manager responsible for the business area in which the breach has occurred. Convene a proportionate breach response team to carry out related actions. Consider representation from communications, HR and IT. Take any immediate steps to prevent any further breach of the same data. Ie. Suspending processing activity. Consider informing JIMU.

2) Assessment of ongoing risk	What type of data is involved? How sensitive is it? Remember that some data is sensitive because of its very personal nature while other data types are sensitive because of what might happen if it is misused Are there any protections in place such as encryption? What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk What could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people How many individuals' personal data are affected by the breach? Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?	Senior manager to conduct a risk analysis using a likelihood vs impact assessment. Obtain copies of policies, procedures and other documentation relevant to the information. Follow ICO checklist within its guidance in completing assessment. Senior manager to review all available information, and discuss with Data Protection Officer to agree the risk level.

3) Notification of breach	Informing people and organisations that you have experienced a data security breach can be an important element in your breach management strategy. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password? Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.	Complete the ICO data breach notification form, submit only if it meets the ICO threshold of a “serious breach” (Data Protection Officer to advise on this) Complete an entry in the breach notification register. Notify other affected organisations if not already done in step 1. Prepare communications strategy.

4) Evaluation and response	It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience. You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.	Data Protection Officer to work with senior manager and breach response team to review actions of the organization, and to propose changes to policies or procedures. Consider additional training requirements for staff. Consider technical solutions to prevent repeat breach. Hold debrief meeting with affected staff to ensure it is a learning experience.

POLICE & CRIME COMMISSIONER

Serving
Hampshire
Isle of Wight
Portsmouth
Southampton

Data Protection Breach Notification Form

Please provide as much information as possible. If you don't know the answer, or you are waiting on completion of an internal investigation, please state this.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. **Details of the data protection breach**

a) Describe the incident in as much detail as possible

b) When did the incident happen?

c) How did the incident happen?

d) What measures have been put in place to prevent an incident of this nature occurring? Please explain in detail

e) What policies, procedures or agreements are considered relevant to this incident?

2. **Personal data placed at risk**

a) What personal data has been placed at risk - Please specify if any financial or sensitive personal data has been affected and provide details below

b) How many individuals have been affected?

c) Are the affected individuals aware that the incident has occurred? Yes / No

d) What are the potential consequences and adverse effects on those individuals / personnel?

e) Have any affected individuals complained to the ICO about the incident? Yes / No / Unknown.

3. **Containment and recovery**

a) What action has been taken to minimise/mitigate the effect on the affected individuals? Please provide details.

b) Has the data placed at risk been recovered? If so, please provide details of how and when this occurred.

c) What steps have been taken to prevent a recurrence of this incident?

4. **Miscellaneous**

a) Do we need to notify any other (overseas), third parties of the data protection authorities about this incident? If yes please provide details

b) Does Hampshire Constabulary need to be informed about this incident? If so, please provide details.

c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

d) Has there been any media coverage of the incident? If so, please provide details of this

WHEN COMPLETED, SUBMIT THIS FORM TO THE DATA PROTECTION OFFICER