Personal Data Breach Policy and Procedures

Version: 8.4

Published: 27/03/2020

DOCUMENT CONTROL

Approval Table

Authority	Name / Role
Author	David Fasanya / Data Protection and Information Manager
Document can be reviewed by	Information Governance Officer
Document can be approved by	Executive Management Team

Document Identification

Document Title	Data Breach Policy and Procedure
Version Number	8.4
Date:	27/03/2020
Total Number of Pages:	14
Security Marking	OFFICIAL

Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
8.0	01/02/2019	DF	JR	Internally reviewed and circulated
8.1	04/02/2019	RLC	DF	Amendments to formatting
8.2	13/02/2019		JR	Amendments to formatting
8.3	22/03/2019	JR	JR	Links to other policies added
8.4	27/03/2020	MAH	JR	Amendments to Data Breach Reporting Form and minor amendments to text.

Contents

1. Introduction

1.1. The Police and Crime Commissioner for West Yorkshire as a data controller processes, collects, holds, and shares personal data. Under data protection legislation (GDPR and Data Protection Act 2018) the Office of the Police and Crime Commissioner (OPCC) is expected to implement institutional mechanisms that can ensure the protection of personal data.

1.2. Technical and organisational measures must be implemented and embedded into day-to-day activities in order to protect personal data from breaches and from incidents of omission (not doing something) or commission (doing something) that can compromise security of data.

1.3. In the event of a compromise of the confidentiality, integrity, or availability of personal data, this can result in potential harm to individual(s), reputational damage, regulatory noncompliance, loss of income and/or punitive financial fines from regulators.

2. Purpose and Scope

2.1. This policy outlines the steps to be followed to ensure an efficient approach in the event of a personal data breach and/or information security incidents within the OPCC.

2.2. This policy relates to all identified or identifiable personal data (e.g name, online identifier, ID number) confidential data, criminal offence data and special categories of data (eg race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health or sexual orientation) that is in the possession of or processed by or on behalf of the OPCC.

2.3. This policy applies to all staff of the OPCC and includes agency staff, temporary staff, contractors, consultants and suppliers and also applies to data processors working for or on behalf of the OPCC. Prevention of breaches has been addressed in the information security policy as adopted from West Yorkshire Police. The objective of this breach policy is to mitigate any personal information breaches and outline the actions necessary in the event of a breach of personal data.

3. Definitions / Types of personal information breach

3.1. For clarity, the following terms are defined:

- Personal data is information that relates to an identified or identifiable individual through unique identifiers such as a name, online identifier, ID number, reference number or other specific factors like social, economic or physical identities.
- Information Assets: Data, software, hardware, component or mobile devices that support information-related activities for a specific area of business.
- Information Asset Owner: Senior members of staff involved in managing the information assets related to a specific area of business.
- Data Controller: A person, public authority, agency or other body which (either alone or jointly with others) determines and exercises control over the purposes and means of processing personal data.
- Data Processor: A person, public authority, agency or other body, which processes personal data on behalf of the data controller.

3.2. A 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, held or otherwise processed by the OPCC.

3.3. Data Breaches are broken down into three types.

- Confidentiality breach:
  Where there is unauthorised or accidental disclosure or access to personal data.
- Integrity breach:
  Where there is an unauthorised or accidental alteration of personal data.
- Availability breach:
  Where there is an accidental or unauthorised loss of access to or destruction of personal data.

3.4. A personal data security breach also extends to both confirmed and suspected incidents. A security incident refers to an event or action that could by commission (by doing something) or omission (by not doing something), compromise the integrity, confidentiality or availability of data or systems and that can potentially damage the data assets or the reputation of the OPCC. Security incidents may or may not involve personal data.

3.5. A security incident can include but is not restricted to the following:

- Theft or loss of personal, confidential or sensitive data or the equipment on which the data are stored such as tablets, phones, USB sticks, laptops or paper records.
- Systems or equipment theft or failure.
- Unauthorised access to use or modification of data and information assets.
- Failed and successful attempts to gain unauthorised access to information assets.
- Unauthorised or accidental disclosure of personal and sensitive data.
- Unauthorised, accidental or unprofessional destruction of data.
- Hacking, denial of service, deliberate destruction or defacement of websites or information assets.
- Human error and non-envisaged incidents such as a fire, flood or other natural disasters.
- Tricking offences where access to information assets are obtained through the deception of the organisation holding it.

4. Security Incident Reporting & Data Breach Reporting

4.1. Any person who accesses, uses or manages OPCC information is responsible for reporting personal data breaches and information security incidents immediately to the Data Protection Officer (DPO) in the OPCC and at the following e-mail address:

DPO@westyorkshire.pcc.pnn.gov.uk

4.2. If a personal data breach occurs outside normal working hours, then it must be reported as soon as practicable. Outside of office hours, further reasonable measures should be taken by the concerned Information Asset Owner to contain the breach and limit its effects pending when the DPO can be reached.

4.3. An Incident Report Form (Appendix 1) available here should be completed by the person reporting the incident. The form should provide as much relevant and accurate information as possible. It should also clarify if any personal data are involved. When fully completed, the Incident Report Form should be submitted to the DPO. The Information Governance Officer will collate records of Data Breaches.

4.4. All authorised persons accessing and processing OPCC data should be aware that any breach of data protection legislation can result in disciplinary measures being initiated against that person, based on the disciplinary policy of the OPCC.

5. Control, Remediation, Investigation and Assessment

5.1. The DPO or Information Governance Officer (IGO) will determine if the personal data breach is still in progress and, in this case, further appropriate steps will be taken immediately to minimise any effects of the breach, establish severity, recover losses and investigate cause and effects.

5.2. The DPO or IGO will determine those who may need to be notified, in addition to any notifications that have already been made in light of any contractual obligations or operational expectations, as based on initial containment plans.

5.3. It is expected that those working in an operational context may need to take immediate steps to contain, manage and communicate with consumers of their service.

5.4. Advice from data protection and other relevant subject matter experts across the OPCC will be sought in resolving incidents and to determine suitable actions for incident resolution.

5.5. All organisations have a duty to report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. On this basis, an investigation will be commenced by the Data Protection Officer or Information Governance Officer as soon as possible and if practicable, within a maximum of 24 hours of the discovery and reporting of the personal data breach.

5.6. The DPO or IGO or other designated officer will investigate the personal data breach and also assess all associated risks, adverse effects, severity and likelihood of occurrence.

5.7. The investigation will consider the following:

- Type of data involved and sensitivity
- The level of protection (e.g. encryptions)

- Exactly what happened to the data (e.g. theft or loss)
- Any evidence of illegal or inappropriate use of the data
- Data subject(s) impacted by the breach, number of persons, potential impact or scope for misuse
- Effects on information assets and broader consequences of the personal data breach.

6. Personal Data Breach Notification

6.1. The DPO will determine if the Information Commissioner's Office (ICO) will need to be notified of the personal data breach and in this case will notify the ICO immediately no later than 72 hours of becoming aware of the personal data breach or as soon as practicable.

6.2. All incidents are to be assessed on a case-by-case basis but the following will also be considered:

- If the breach will be likely to result in a high risk of adversely affecting individual rights and freedoms.
- If notification of the data subjects would help the individual(s) affected to mitigate the risk and further help to prevent unauthorised or unlawful use of their personal data.
- If there are any legal / contractual notification requirements or any dangers of over notification - as not all incidents require notification, which in this case can cause inconsistent enquiries and unnecessary work.
- Is it necessary to contact individuals whose personal data has been affected by the incident i.e., where it has been established that the breach will result in a high risk to their rights and freedoms.
- How to prepare the notification with details of how and when the breach occurred, the data involved, clear advice on protecting themselves, and actions taken to mitigate the risks.
- How affected individuals can contact the OPCC for further information or to ask questions.
- If there is evidence of illegal activity or related risks, the DPO will notify third parties such as the police, insurers, banks or credit card companies, and trade unions.
- If the OPCC communications staff should be informed regarding press releases and the handling of press enquiries.
- If a record will be kept of any personal data breach, regardless of whether notification was required.
- Obtaining legal advice, depending on the severity of the breach.

7. Evaluation and response

7.1. After incident containment, a full review of the personal data breach causes, response effectiveness, controls, corrective actions, policies and procedures will be conducted by the Data Protection Officer or Information Governance Officer and will be reported to the Executive Management Team in the OPCC and the PCC.

7.2. The review will consider the following amongst others:

- Location of personal data, storage, access control and security.
- Identification of weakest security points and the biggest risks.
- Data transmission and minimisation processes.

- Personnel training and awareness.
- Data breach plans and responses to reported breaches.
- Recommendations on required adjustments to processes, policies, procedures and systems will be implemented by the concerned information asset owner(s).
- Records relating to the review will be retained in accordance with the retention and disposal policy and legislative requirements.

7.3. An analysis of data breaches reported to the OPCC will be provided to Joint Audit and Ethics Committee annually.

8. Policy Updates & Review

8.1. This policy will be updated as required for adhering to current data protection legislation and compliance, but in any event no later than three years.

9. Legislative compliance

9.1. This Policy complies with the following legislation and guidance:

- General Data Protection Regulation (GDPR).
- Data Protection Act (DPA) 2018.
- Computer Misuse Act 1990.
- Code of Practice on the Management of Police Information (MOPI) and Supporting Guidance.

10. Links to other Policies

10.1 The OPCC has adopted the same information management policies as West Yorkshire Police, including:

- Computer Use Police
- Information Security Policy
- Protective Marking Scheme
- Universal Serial Bus Devices (USB)

APPENDIX 1 – SECURITY INCIDENT REPORTING FORM

You must immediately report any breach of personal data or information asset as soon as you discover the breach and notify the data protection unit of the OPCC by completing this form and sending it by email to: DPO@westyorkshire.pcc.pnn.gov.uk

Form 1: Security Incident Breach Notification **(To be completed by the person reporting the incident)**	
Date and time of incident discovery	
Date and time of actual incident (if known)	
Location of the incident	
Name of person reporting the incident	
Contact details of person reporting the incident (Email & phone number)	
Short description of the breach incident and data affected, including whether any personal information is involved.	
Total number of data subjects involved in breach (if known)	
If any personal data has been breached, describe the type of personal information involved e.g. Name, address, email, law enforcement, conviction data, health data, biometric, ethnicity, sexuality.	

Detail any action taken to recover or secure the data.	
To be completed by OPCC DPO or IGO	
Received by	
Date and Time Received	
Immediate Action(s) Taken	
Date of Action(s) Taken	
Has a Data Breach Occurred?	

Form 2: Security Incident Severity Assessment **(Completed by the OPCC DPO or IGO)**	
Incident number	
Severity Assessment completed by	
Date and time of report	
Details of Information Assets involved in the incident.	
Is this incident a Data Breach, Security Incident or Near Miss?	
Type of data breach: Confidentiality, Integrity or Availability.	
Detail and nature of the data lost or put at risk due to the breach/ incident Please delete as appropriate	• Name • Email/ IP address • Telephone number • Postal address • Financial Information • Personal information related to children or vulnerable adults • HR Profiles and Work performance details • Personal security and safety information. • Law Enforcement Data • Special category data: o Racial or Ethnic o Health/ Biometric & Genetic data o Political Opinions o Sexuality o Trade Union Membership o Religious Beliefs
Number of Data Subjects affected.	
Details of contractual security arrangements related to the breached data	

Detail immediate action taken to recover the data, mitigate the consequences to the data subjects or secure data in event of a security incident.	
Estimated consequences of the data loss to the data subject in terms of their rights and freedoms.	
Estimated consequences of the data loss to the OPCC in terms of adverse effects relating to legal, reputational, financial or operational impacts.	
Comments on breach assessment, Recommendations	

Follow up action(s) and responsible person	
Details of other internal stakeholders who have been notified of the incident	

Notification and Lessons Learnt	
Is notification to the Information Commissioners Office (ICO) required? (include rationale)	
Notification date and time if yes to the above	
Was notification within 72 hours?	
If notification was not within 72 hours then state reasons	
Is notification to the concerned data subjects required? (include rationale)	
If yes to the above then state the notification date	
Is notification to other external regulators or stakeholders required? (include rationale)	
If yes to the above, state the external regulators and stakeholders notified	
Notification date if yes to the above	

Identify any lessons learned from this breach and subsequent investigation.
Identify and confirm what changes have been implemented in light of this breach and subsequent investigation.