STANDARD OPERATING PROCEDURES:
OFFICE OF THE BEDFORDSHIRE POLICE AND CRIME COMMISSIONER

Title	Data Breach Management Policy
Area of Compliance	Compliance
Version No.	2.0
Senior Lead	Head of Governance and Transparency
Author	Compliance

Revision History

Date	Revision	Change	Section	Review Date
21.05.2018	1.0			21.05.2019
21.05.2019	1.0	No Change		21.05.2020
20.09.2019	1.0	No Change		20.09.2020
20.09.2020	1.0	No Change		20.09.2021
20.09.2021	1.0	No Change		20.09.2022
17.10.2022	2.0	ICO email updated, details for Data Protection Lead Officer and Data Protection Officer		20.09.2023

Introduction

The Office of the Police and Crime Commissioner are committed to ensuring appropriate measures are taken against any information security threat/incident and data breach aimed to compromise the confidentiality, integrity and availability of the police information including government classified and personal data as defined by the General Data Protection Regulation (GDPR) & Data Protection Act 2018 (DPA18). BCH will also react appropriately and proportionately to bring the situation within appropriate control.

Identifying and assessing a personal data breach is important in reducing risk. Reporting breaches to the Information Commissioners Office (ICO) becomes mandatory within 72 hours under GDPR and can be reported by the Police and Crime Commissioner, the Data Protection Lead Officer (DPLO), the Data Protection Officer (DPO) or a member of the OPCC staff team who have reasonable cause to believe that there has been a breach in personal data.

The ICO describe a personal data breach as:

> *A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. 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.*

This 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*
- *Loss of availability of personal data*

All breaches in relation to personal data will be reported to the ICO within 72 hours and recorded on the Reporting Breaches log.

Examples of a breach

The main examples of a breach of information that may occur in the OPCC are:

- Forwarding an e-mail outside the OPCC which includes personal e-mail addresses from someone who has not given their consent to have their e-mail shared
- Providing personal information outside the OPCC
- Loss of sensitive documents e.g., leaving a document marked 'official sensitive' or higher level of security in a public place
- Having a force lap-top or phone which contains, or has access to, sensitive or personal information stolen

This is not an exhaustive list.

Reporting process

The Head of Governance and Transparency should be notified immediately if a personal data breach is suspected. They should be given any evidence in relation to the breach and may seek clarification of the law from professionals. They will consider the material significance of the breach, taking into account its cause, effect, the reaction to it, and its wider implications, including (where appropriate) dialogue with the Police and Crime Commissioner.

If the Head of Governance and Transparency is not available, the DPO or any other OPCC staff member may report and record the breach.

When reporting a breach, you need to consider the following:

- Potential detriment to individuals
- Volume of data affected
- Sensitivity of data

The method of reporting is currently started with filling in a Security Incident Form. It is then emailed to Info Security (IAU) whereby a member of the IAU team will action the incident and record it and make an initial assessment. A running log will be kept of all action taken, and regular updates to this log will be made by the IAU team members.

The **first 72 hours after you become aware of a data breach are critical**. This is the deadline given to organisations under the Data Protection Act 2018 to report information security incidents to the Information Commissioners' Office (ICO).

However, not all breaches need to be reported to the ICO. Data breaches only need to be reported if they "pose a risk to the rights and freedoms of natural living persons". This generally refers to the possibility of affected individuals facing economic or social damage, such as discrimination, reputational damage, or financial losses. Most breaches fit into this category, but not all. For example, if the information can't be linked to a specific individual, there's likely to be very little risk to the 'rights and freedoms of an individual'.

The Information Commissioners Office reporting process:

Breaches must be reported to the ICO using their 'Reporting Breaches' process, see https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ and use their 'reporting a personal data breach notification form', providing as much information as possible. Send the form to icocasework@ico.org.uk or for help or advice, ring their helpline on 0303 123 1113.

When reporting the breach, you need to include the following information:

- Data controller's name: **Office of the Police and Crime Commissioner for Bedfordshire**
- Data Protection Lead Officer for OPCC: **Head of Governance and Transparency, Katie Beaumont**
- Data Protection Officer: **BCH Information Governance Manager, Jolene Neil**
- Data controller's address: **OPCC, Bridgebury House, Bedfordshire Police Headquarters, Woburn Road, Kempston, Bedford MK43 9AX**
- Who the ICO should contact if they require further details concerning the incident
- Details of the breach, including a description of the nature of the breach, the categories and approx. number of individuals concerned, and the categories and approx. number of personal data records concerned.
- Description of the likely consequences and of the measures taken, or proposed to be taken, to deal with the breach, including where appropriate, the measures taken to mitigate any possible adverse effects.

If the breach is likely to adversely affect the personal data or privacy of an individual, you must notify the individual of the breach without unnecessary delay and give them the following information:

- Your name and contact details
- The estimated date of the breach
- A summary of the incident
- The nature and content of the personal data
- The likely effect on the individual

- Any measures you have taken to address the breach; and
- How they can mitigate an possible adverse impact

You do not have to tell individuals of a breach if you can demonstrate the data was encrypted but the ICO can require you to do so if they consider the breach is likely to adversely affect the individual.

If the personal information was originally received via a 3rd party, the 3rd party should also be notified of the data breach.

Record the date and nature of the breach and action taken on the **Reporting Breaches Log**, which can be found in the OPCC GDPR Folder.

Bedfordshire OPCC link with BCH (Beds, Cambs, Herts) Information Management Unit when dealing with Information management – BCH16/006 Information Security Incident and Data Breach Management Procedure are available on the intranet.