**Personal Data Breach Reporting**

In line with General Data Processing Regulation (GDPR), as a Commissioned Provider for the Policing, Fire and Crime Directorate (PFC) of the York and North Yorkshire Combined Authority (YNYCA) there are some additional responsibilities in relation to reporting data breaches that you need to be aware of, to assist us in complying with the legislation.

All organisations have a duty to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach.

**What is a personal data breach?**

According to the Information Commissioner’s Office (ICO), a personal data breach means 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.

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, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

It is the data controller’s responsibility to report data breaches to the ICO within the allocated timeframes.As a Commissioned Provider for PFC, your timely reporting of a breach is crucial to enable us to report to the ICO within the allocated timeframes.

**As a Commissioned Provider for PFC, you must complete and submit the form below within 24 hours of any data breach relating to the services you provide on behalf of the PFC.**

For further guidance and information, please visit the ICO website:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

**Policing, Fire and Crime Commissioned Providers Data Breach Reporting Form**

**This form must be submitted within 24 hours of any data breach to your Commissioning and Partnerships Manager who will forward this accordingly.**

|  |  |
| --- | --- |
| **Reporting Organisation** |  |
| **Incident Date and Time** |  |
| **Reporting Date and Time** |  |
| **Reported by (Name & Job title)** | **Contact Telephone Number:**  |
| **Email Address:**  |
| **Incident location** |  |
| **Incident details and actions taken** *(please provide as much information as you can to ease the handling of the incident)* |  |
| **Please give as much description of the nature of the personal data breach, including number of individuals concerned** |  |
| **Categories (e.g staff, victims, suspects, convicted) and approx. number of people concerned** |  |
| **Categories and approx. number of personal data records concerned** |  |