



This document is shared as a for information example.

Auditing of LEDS data access and usage

Why?

Accountability is a requirement under the Data Protection Act 2018, which also acts in accordance with GDPR. The General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), which deals with the processing of personal data by data controllers for 'law enforcement purposes', took effect from 25th May 2018. To comply with it, organisations must evidence that their data protection measures are sufficient. They must have appropriate technical and organisational procedures, which include keeping sufficient records of their processing activities.

What?

An audit is a systematic, independent examination of organisation processes, systems and data to determine whether activities involving the processing, use and sharing of the data are being carried out in accordance with the Data Protection Act 2018.

Further Guidance

Authorised Professional Practice (APP) on Audit for Data Protection is developed and owned by the College of Policing. Police services who are accessing LEDS should adhere to this guidance. Other Law Enforcement Agencies can access the APP document and use this as guidance in developing their own internal standards. The Code of Connections will also serve to provide organisations with some guidance on expected audit practice.

What do we need to do to meet this requirement?

The Home Office is responsible for:

- Building into the system the technical capability for logging access so as to allow those with the responsibility for conducting audit to subsequently make such checks
- Proactively lead organisations to put in place measures to protect LEDS as a national asset and mitigate the risk of corruption
- Conducting audit checks at a national level, by delegation to the National Systems Audit Team, to proactively drive compliance and support the investigation of malpractice.
- Collecting and reporting data on compliance with LEDS best practice guidance, breaches of LEDS (and PNC/PND) integrity and the outcomes of disciplinary procedures.
- Providing and updating strategic and policy guidance across national and local information systems, to help data owners mitigate and manage risk in a timely manner

The organisation will be responsible for:

- Appointing a senior manager, a Senior Information Risk Officer (SIRO) or Data Protection Officer, who is responsible for the strategic audit programme and has responsibility for compliance with audit across the organisation

- Confirming that people who have an identified business need to access the system in order to carry out their current role are those who have access
- Ensuring that unlawful access or use of information held on the system can be identified.
- Ensuring that procedures are in place to address and report unlawful access or use of information by individuals who act outside of the Code of Practice
- Ensuring that there is a systematic process for conducting regular audit checks and reviewing audit logs that confirm that access to the Law Enforcement Database is limited to those with authority to access the system and to ensure such access is both lawful and reasonable.
- Ensure that monitoring and dip-sampling of the work of those who enter and maintain data is carried out in line with practice guidance and the results collated and reported
- Compiling organisational audit reports, including findings and recommendations and action plans detailing how findings and recommendations have been addressed to ensure that any risk has been mitigated
- Providing evidence of audits and their outcomes for external audit and inspection purpose, for example, an inspection by Her Majesty's Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS)
- Ensuring that updated guidance is disseminated to relevant managers and staff within the organisation to ensure that practice remains valid in line with current national guidelines

As an operational manager within the organisation you will be responsible for;

- Confirming that people who have an identified business need to access the system in order to carry out their current role are those who have been trained, and records of training and CPD are available
- Confirming that people who have an identified business need are adhering to Code of Practice guidance for access and use of data and that records are maintained of their access
- Monitoring and dip-sampling the work of those who enter and maintain data to ensure information is accurate, relevant and up to date
- Ensuring that updated guidance is disseminated to, and understood by, relevant staff within the organisation to ensure that practice remains valid in line with current national guidelines

As a LEDS user you are responsible for;

- Complying with all system access requirements of the organisation
- Ensuring that access to the system is justified and is only carried out for a lawful purpose
- Ensuring that accurate information on justification for a system check is applied upon access
- Keeping personal skills levels up to date by adopting an active continuous professional development approach, accessing refresher training, proactively checking for system and legislation updates and reading technical guidance