

**Equality and Human Rights Impact Assessment (EqHRIA)**

# Summary of Results

## Policy/Practice Name:

Lawful Business Monitoring National Guidance

## Owning Department:

Professional Standards Department

## Date EqHRIA Completed:

13/10/2022

## Purpose of Policy/Practice:

The purpose of this document is to provide information on what Lawful Business Monitoring (LBM) is, and why it is used. Its usage is restricted to ACU staff along with a select few staff members from PSD. The usage element will only apply to specific officers and staff, however it is important to highlight that all of Police Scotland assets are monitored by LBM. This is documented below.

Lawful Business Monitoring is an auditing tool which came into use on Monday 25 January 2021 following a recommendation from HMICS. Its use assists the Force in the protection of its staff, information assets and data. It is also intended to assist in the investigation of criminal and corrupt activity. The system monitors and records all computer-based actions of all Police Scotland employees who use any element of the Force IT infrastructure and associated networks.

## Summary of Analysis / Decisions:

### What the assessment found, and actions already taken.

The assessment found that the likely impact on the protected characteristics was determined to have no impact on the following protected characteristics:

Age, Disability, Sex, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion or Belief and Sexual Orientation.

Presently, there has been no evidence received as a result of Police Scotland’s previous consultation or consultations carried out throughout the United Kingdom that these protected characteristics would be impacted by LBM.

A positive / high impact was assessed overall given that the project involves the processing of personal data for the purpose of auditing users of police systems. The data will be collected from all parties which have access to the Police Scotland Network. This data is collected from workstations, laptops and mobile devices and is collected 24/7, every day of the year on a continuous and ongoing basis. It is worthy to note that the system does not differentiate between “Force use” and “personal use”, and so some data the user considers to be “private” may be captured and processed by the system. Any personal data deemed to be irrelevant to investigations will ultimately be disregarded. Whilst the individual’s protected characteristics were assessed as no impact, a positive/high impact overall was found due to data being collected from all parties which have access to Police Scotland Network.

In respect of Article 7, this Article will be protected as it states that public authorities must explain clearly what counts as a criminal offence so that you know when you are breaking the law. The Guidance document and Acceptable Use Policy will set out the expectations for staff and provide details of what actions could result in criminal charges. The justification behind this includes investigation of crime or corrupt activity, mitigation of the threat of internal corruption and the safeguarding of the reputation of Police Scotland.

In respect of Article 8, it is accepted that as with any investigative technique there may be collateral intrusion. This includes the unintentional discovery of sensitive data, personal information and other material not relevant to the investigation. In addition, all data received will be extensively researched and analysed to ensure that it is relevant to this investigation. Data found to be irrelevant will be disregarded.

In all cases Lawful Business Monitoring will only be utilised where necessary, justified and proportionate to prevent and detect crime and corrupt activity. The decision and rational for the use of LBM is to be clearly documented within an investigation detailing the suspected criminality or corrupt activity and the benefits of using the software.

External requests for data and dissemination will take place in accordance with intelligence handling requirements, data protection considerations and proportionality in terms of the purpose for which the LBM data is required. Section 46 of The Investigatory Powers Act 2016 permits businesses, including public authorities, to monitor, intercept and record electronic communications transmitted through equipment provided to conduct business. However, Police Scotland has a legal obligation to control protected information, and this must be strictly adhered to.

As communications will be recorded and may be monitored, there can be no expectation of privacy at any time when using Police Scotland devices and systems. There are SOPs / Guidance in place to advise how systems should / should not be used, Network Users have some discretion whether they decide to follow these rules and complete control over what they choose to disclose in relation to their own personal life.

The guidance will prevent, so far as possible, interference with Article 8 except in fully justified circumstances to detect and prevent crime. Data found to be irrelevant to any investigation will be disregarded:

The Police Service of Scotland (Conduct) Regulations 2013

The Police Service of Scotland (Conduct) Regulations 2014

The Disciplinary (Authority / Police Staff) SOP for SPA / Police Staff.

The Investigatory Powers Act 2016 (Section 46)

The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018

## Summary of Mitigation Actions:

### What the assessment found, and actions already taken.

If your assessment identified any actions required to mitigate impact, provide details of what actions were identified and how these will be monitored or reviewed.

Mitigation:

The guidance will prevent, so far as possible, interference with Article 8 except in fully justified circumstances to detect and prevent crime. Data found to be irrelevant to any investigation will be disregarded.

* The Police Service of Scotland (Conduct) Regulations 2013
* The Police Service of Scotland (Conduct) Regulations 2014
* The Disciplinary (Authority / Police Staff) SOP for SPA / Police Staff.
* The Investigatory Powers Act 2016 (Section 46)
* The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018

The document will hereafter be reviewed on a yearly basis and will be subject to review by Information Assurance. The documents will be updated as and when required to ensure continued compliance on behalf of the Anti-Corruption Unit.