ORKNEY
ISLANDS COUNCIL

RIPSA Data Safeguards Compliance Process

All our written information can be made available, on request, in a range of different formats and languages. If you would like this document in any other language or format, please contact Strategy, Performance and Business Solutions on 01856873535 or email spbs@orkney.gov.uk

Contents

1. Introduction

1.1.

This document sets out Orkney Islands Council's process to safeguard data security regarding information gathered which falls within the framework of the Regulation of Investigatory Powers (Scotland) Act 2000 [RIPSA] and the Investigatory Powers Act 2016 ('the Acts').

1.2.

Reference is made to Orkney Islands Council's policies and procedures in respect of covert surveillance and use of covert human intelligence sources (hereinafter collectively referred to as 'the Council's RIPSA policies and procedures'), to which this process is subsidiary.

1.3.

This Data Protection Compliance Process is supplemental to the safeguards contained in Chapter 8 of the Covert Surveillance and Property Interference: Code of Practice and in Chapter 8 of the Covert Human Intelligence Sources: Code of Practice issued by the Scottish Government on 20 December 2017 and, in the case of any conflict, these Codes would prevail.

2. Objective

2.1.

The objective of this Process is to ensure that all data obtained through processes subject to the Regulation of Investigatory Powers (Scotland) Act 2000 is maintained in a safe, secure, and effective way.

2.2.

The procedure will set out a retention, review and destruction process to ensure that information obtained is not kept for any longer than is required.

3. Data Safeguards

3.1.

Any information obtained through surveillance should be handled in accordance with the safeguards that the Council has put in place to support data protection, as set out in the Council's Data Protection Policy and Procedure for Staff, which can be found here.

3.2.

The following should be undertaken to ensure the integrity of data:

- Ensure that the information you hold is relevant and that data is accurate and up to date.

- Any data collected or transported off site should be kept secure, and that authorisation has been obtained to do so.
- Ensure that any paper-based files are stored securely, such as in access controlled areas / locked filing cabinets etc. to minimise risk of theft or loss.
- Ensure that information you are working with cannot be accidentally overseen by anyone else, follow a clean desk policy.
- Ensure any breaches are reported to the Information Governance Officer as soon as you are aware of them.
- If a member of the public makes a request for their data ensure this is forwarded to foi@orkney.gov.uk.

4. Records Management

4.1.

The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections within Services and a Central Register of all Authorisation Forms will be maintained and monitored by Legal and Governance.

4.2.

Each authorisation will be allocated a unique reference number which will be linked to information obtained through the use of the regulated powers.

4.3.

Any material obtained using powers under the Regulation of Investigatory Powers (Scotland) Act 2000 should form part of an investigation file and a retention period set (see section 5 below) to record how material will be handled. Legal and Governance will oversee this process for files and dispose of them appropriately.

4.4.

Information that should be retained within the records should be:

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer.
- A record of the period over which the surveillance has taken place.
- The frequency of reviews prescribed by the Authorising Officer.
- A record of the result of each review of the authorisation.
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested.
- The date and time when any instruction was given by the Authorising Officer.
- The Unique Reference Number for the authorisation (URN).

4.5.

Information obtained through surveillance should be held separately so that it is easily identifiable and scheduled for deletion or destruction in line with the Council’s Retention Policy.

4.6.

This record must be regularly updated whenever an authorisation is granted, renewed or cancelled. This will be achieved by the Authorising Officer forwarding a copy of the approved application, renewal or cancellation to the Head of Legal and Governance for the centrally retrievable record.

4.7.

An access controlled Microsoft Teams site with a closed group should be set up in order to manage access to an electronic information file relating to a RIPSA application, and limit dissemination, copying and retention of material to the minimum necessary for the authorised purposes.

5. Retention

5.1.

Orkney Islands Council holds a formal retention schedule. For both covert surveillance and covert human intelligence sources, data should only be retained for a maximum of three years.

5.2.

Once the retention period is reached the file should be scheduled for deletion or secure destruction in line with the Council’s Retention Policy.

5.3.

For electronically held records (Microsoft Teams or Electronic Document and Records Management System) automated retention labelling and automatic disposal rules can be set to ensure that information is not retained longer than necessary.

5.4.

Periodic reviews should be undertaken to ascertain whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, retained data should be duly disposed of.

Document Control Sheet

Review/Approval History

Date	Name	Position	Version Approved
9 October 2023	Gavin Mitchell	Head of Legal & Governance	V .1

Change Record Table

Date	Author	Version	Status	Reason