Intervention Procedures

Internal management procedures

Scottish Information Commissioner

Contents

Glossary and abbreviations

Term used	Explanation
The Commissioner	The Scottish Information Commissioner
FOISA	Freedom of Information (Scotland) Act 2002
EIRs	Environmental Information (Scotland) Regulations 2004
FOI	FOISA and the EIRs
Codes of Practice	Scottish Ministers' Code of Practice on the discharge of functions by Scottish public authorities under FOISA and the EIRs; Scottish Ministers' Code of Practice on records management by Scottish public authorities under FOISA
IP	Intervention Plan
SIC	Scottish Information Commissioner

Introduction

1. Both the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 (FOI) give the Commissioner the power to act where a public authority is not complying with FOI or with the Scottish Ministers' Codes of Practice. These powers include:

   (i) promoting good practice

   (ii) assessing whether an authority is following good practice

   (iii) issuing practice recommendations where it appears to the Commissioner that an authority is not complying with the Codes of Practice

   (iv) issuing enforcement notices where the Commissioner is satisfied that a public authority has failed to comply with FOI law.

2. Separately, the Commissioner has a duty, on receipt of an application, to investigate whether a public authority has dealt with an information request in accordance with FOI. That work is subject to separate procedures – see the Investigations Handbook. The Commissioner's Intervention Procedures reflect the action which the Commissioner will take proactively ("an intervention") to improve public authority practice more generally.

3. The Commissioner's Enforcement Policy (VC36119) sets out the Commissioner's policy on what will be enforced and the outcomes that enforcement aims to achieve.

4. The Intervention Procedures (this document) set out in more detail when action will be considered and the procedures that will be followed when undertaking an intervention.

5. Depending on the circumstances of each case, an intervention may be:

   (i) **informal** (recommending the authority resolves a concern) – Level 1

   (ii) **formal**, requiring the authority to make a specified improvement – Levels 2 and 3

   (iii) **formal**, with the issue of an Enforcement Notice or Practice Recommendation – Level 4.

6. These procedures set out:

   (i) how we gather evidence to inform interventions.

   (ii) the criteria we apply to decisions to intervene.

   (iii) intervention activities we may undertake.

   (iv) how we manage interventions.

Evidence

Sources of evidence

7. We routinely record, in our case handling system, any concerns we note in the course of our day to day business. Our Enquiries Procedures and Investigations Handbook set out how these records are created and maintained.

8. We analyse data about FOI requests from a range of sources. These sources include:

(i) data from the Commissioner's decisions

(ii) statistical data provided by Scottish public authorities to the Commissioner's FOI and EIR statistics portal

(iii) quantitative and qualitative data from other sources, including meetings with stakeholders, approaches to the Commissioner by third parties, online request portals and relevant media reports about FOI.

9. Our analysis aims to identify early any of the concerns listed in the Enforcement Policy so that we can intervene as soon as possible.

10. The results of the analysis are reported quarterly to the Commissioner's Investigation Performance Meeting. The quarterly report provides data about:

- All authority and sector trends, including: request volumes, late responses and failures to respond; use of specific provisions; non-compliance concerns; other issues that may warrant intervention (from statistics portal data)
- Non-compliance data (from our case handling system)
- A summary of concerns about individual authority practice.

Decisions to intervene

11. Decisions to intervene are based on evidence of a breach of statutory duty in FOI law or non-compliance with a Code of Practice (as set out in the Enforcement Policy). Most decisions to intervene formally relate to recurrent breaches or non-compliance.

12. The objective of an intervention is to remedy the breach or non-compliance within an acceptable period.

13. Interventions are proportionate to the concern identified and made at the appropriate level to achieve the desired outcome. They may:

Intervention	**Intervention Level**
Alert the authority to a minor concern and may, or may not, recommend it takes action	1
Require the authority to remedy a breach or non-compliance by a given date	2
Require the authority to commit to and deliver an action plan to remedy a breach or non-compliance	3
Lead to issue of a Practice Recommendation or Enforcement Notice	4

14. Interventions may include an assessment phase where appropriate to identify in detail the nature and/or extent of the breach or non-compliance.

Who decides to intervene?

15. Level 1 interventions can be initiated by any member of SIC staff who identifies a concern, without the need for prior agreement of their line manager.

16. A decision to open a level 2 intervention may be taken by:

    (i) The Commissioner

    (ii) The Head of Enforcement or Deputy Heads of Enforcement

    (iii) The Head of Policy and Information

17. A decision to open a level 3 intervention may be taken by the Commissioner or Senior Management Team, usually following a recommendation by:

    (i) The Head of Enforcement

    (ii) The Head of Policy and Information

    (iii) An Investigations Performance Meeting

18. A decision to open a level 4 intervention may only be taken by the Commissioner, usually on the advice of the Head of Enforcement.

19. For interventions at Levels 2, 3 and 4 there will always be a formal record of the decision to intervene and why it was taken. This may take the form of a manager's instruction to an officer or a minute of a meeting at which the decision was taken. This is to be recorded in the relevant case file. See paragraph 20 for advice about recording the decision to respond in a Level 1 case.

Levels of intervention – further detail

Level 1

20. Level 1 interventions aim to remedy minor failures to follow good practice. In these cases, we provide informal advice and assistance to authorities, setting out our concern and suggesting particular action (including any recommended follow-up action) if a relevant failing is identified as a result of an application or enquiry. These are to be recorded in the relevant existing case file.

21. Where there is evidence of a recurring concern which the authority has already been asked to remedy, the matter should always be referred to the immediate line manager to decide whether a Level 2 intervention is appropriate. Where the line manager decides the matter should be dealt with at Level 1, the concern must be raised with the authority and action recommended.

22. Level 1 intervention case files are also used to record compliance observations from casework or failures to submit quarterly statistics and issues with Model Publication Scheme compliance. These records are collated for the monthly interventions reports.

Level 2

23. Level 2 interventions require action by the authority to remedy breaches or non-compliance issues that cannot be resolved by a Level 1 intervention, or which are too serious to be resolved by informal action.

24. A Level 2 case may be opened by the Commissioner, the Head of Enforcement/Policy and Information or a Deputy Head of Enforcement. Day to day management of the case will usually be allocated to an FOIO as the "intervention officer". In some cases, it is appropriate for there to be close supervision of the case throughout by a Deputy Head of Enforcement or

more senior line manager, for example, where the authority has ignored a Level 1 intervention or where the concern needs to be raised with senior managers of the authority or multiple business areas. The intervention officer will be told who the “intervention manager” is; this may change throughout the course of the intervention.

25. Where action is required in a Level 2 intervention, the authority must advise in writing whether or not it has complied with the required action. If it fails to comply with the required action then the case may be escalated to a Level 3 or Level 4 intervention.

Level 3

26. Level 3 interventions require the authority to devise and deliver an action plan (agreed by the SIC)to remedy breaches or non-compliance. This will generally be more appropriate in:

    (i) more serious cases

    (ii) more complex cases where detailed research may be required, or

    (iii) cases where a Level 2 intervention has failed to achieve improvements.

27. These cases are again allocated to one or more investigation officers as the “intervention officer”. Level 3 interventions will almost always be closely supervised by one or more senior managers, who may also call upon the support of other SIC staff in the course of the intervention. The intervention officer will be told who the intervention manager is; this may change throughout the course of the intervention.

28. In most Level 3 cases, the authority will be required to:

    (i) research the causes of the identified areas of concern. This may include asking the authority to complete a relevant self-assessment toolkit module.

    (ii) report the causes to us and/or share the findings of any self-assessment.

    (iii) draft an action plan, setting out measure(s) to remedy the concern.

29. In some, but not all, Level 3 cases, we may conduct a detailed assessment of a particular aspect of an authority’s practice and this may involve:

    (i) requiring the authority to provide information (this may be by means of an Information Notice)

    (ii) visiting the authority to inspect systems or documents

    (iii) meetings or interviews with relevant staff or senior managers of the authority. (Appendix 3: Criminal offences and Appendix 4: Whistleblowing must be read before an interview takes place.)

30. The intervention officer and the intervention manager will agree the authority’s action plan and timeframe for completion. This important stage may be iterative as plans may require significant amendment before they are capable of approval. Where an action plan cannot be agreed with the authority, consideration will be given by the Commissioner to elevating the intervention to Level 4.

31. When the action plan has been agreed, the authority will be asked to implement it as soon as practicable.

32. During the implementation period, the intervention officer and the intervention manager will ask the authority to provide regular updates of progress against the action plan and/or relevant performance data. Failure to implement the plan or improve performance may result in a decision being taken by the Commissioner to elevate the intervention to Level 4.

Level 4

33. Level 4 interventions generally address serious or consistent concerns, or cases of repeated breaches, and may also be used in the event of a refusal to comply with FOI law or the Codes of Practice. These interventions are often, but not exclusively, in the context of previous interventions by the Commissioner, particularly where lower levels of intervention have not been successful or complied with.

34. These cases are again allocated to one or more intervention officers. Level 4 interventions will almost always be closely supervised by one or more senior managers, including the Commissioner, who may also call upon the support of other SIC staff in the course of the intervention. The intervention officer will be told who the intervention manager is; this may change throughout the course of the intervention.

35. In these cases, the Commissioner may:

    (i) decide to carry out an on-site assessment of an authority's practice, including on-site assessment as set out in paragraph 27 above;

    (ii) issue (or give warning of our intention to issue) a Practice Recommendation in terms of section 44 of FOISA specifying the steps that an authority must take in order to conform with the Codes of Practice;

    (iii) issue (or give warning of our intention to issue) an Enforcement Notice under section 51 of FOISA requiring an authority to take specified steps to comply with Part 1 of FOISA or with the EIRs.

Process for formal interventions (Levels 2, 3 and 4)

36. Formal interventions involve the following steps:

- Setting up the case file
- Case allocation to an intervention officer
- Further research
- Intervention plan
- Monitoring progress
- Review
- Closing an intervention
- Internal reporting

37. Each of these steps is described in detail below.

Setting up the case file

38. The intervention manager will open a new intervention case file in the case management system. The public authority data and the following fields in the Intervention tab must be added/completed:

    (i) Date

    (ii) Raised by

    (iii) Intervention type

    (iv) Area of concern

    (v) Synopsis

    (vi) Related to Case

    (vii) Is follow up response from public authority required?

39. The intervention manager must also add all relevant background information to the Documents section. This must include, where relevant, a copy of the quarterly report to the Investigations Performance Meeting which identified the concern.

Case allocation to an intervention officer

40. Where the case is to be transferred to an intervention officer for day to day management, the intervention manager will send a written instruction to the intervention officer at the same time as transferring the case. The written instruction should set out:

    (i) the level of the intervention

    (ii) details of the concerns/breach identified

    (iii) a precis of the evidence for those concerns

    (iv) an instruction on whether the manager considers that an assessment phase is required, and if so what degree of assessment is considered appropriate

    (v) a timeline for preparation of a draft intervention plan

    (vi) the names of any other colleagues to be involved in the intervention.

41. From this point, the intervention officer is responsible for maintaining and updating the case file. This includes:

    (i) Updating the Status box in the case workflow to reflect changes:

    - Initial contact: includes assessment (by authority or by SIC)
    - Action planning: from date of submission of action plan to date agreed
    - Implementation: authority implementing action plan and providing regular updates
    - Monitoring: where we impose an extended period of monitoring following the implementation period.

    (ii) Records management (see Appendix 1: Records management).

Intervention plan

42. Within two weeks of receiving the case, the intervention officer should prepare a draft intervention plan and send it to the intervention manager and any other nominated colleagues. The intervention officer should also convene a case meeting with the intervention manager and nominated colleagues. This meeting should be held within a week of circulating the draft intervention plan.

43. In some cases, we know enough about the practice concern to draft a reasonably full intervention plan. In other cases, we need more information, particularly from the public authority. The development of an intervention plan is often iterative. The aim at the draft stage is to complete the plan as far as possible and, where there is uncertainty, to identify this and the actions that will be taken towards completing the full plan.

44. A completed intervention plan should:

    (i) set out the evidence for making the intervention, including non-compliance reports, statistical reports and research from wider sources.

    (ii) describe the scope and scale of the intervention, confirming whether the intervention is at the appropriate level and defining the practice area(s) to be addressed, with reference to FOI law or the Codes of Practice.

    (iii) Where practicable at this stage, list the proposed targets for improvement to be achieved. These must be Specific, Measurable, Actionable and Realistic. For example, the authority is to:

        (a) Respond on time to 90% of all requests received in the next six month period

        (b) Issue notices compliant with [section X or regulation X] to requests from [specified date]

        (c) Provided full explanations in every refusal for where exemptions or exceptions are applied from [specified date]

    (iv) (generally) also detail:

        (a) The authority's current performance levels (what is giving cause for concern)

        (b) Whether any further assessment is required and what it seeks to establish / achieve

        (c) The proposed actions to be taken by authority / SIC, with timescales

        (d) How progress will be monitored

        (e) Proposed outcome targets

    (v) Reporting – how the intervention will be reported .

    (vi) Timeline – an estimate of how long we expect the intervention will take to achieve the outcome (to be amended if appropriate when the intervention plan is agreed, or dependent on the authority's performance during the intervention)

45. The intervention manager should approve the intervention plan within three weeks of allocating the case. Following that approval, the intervention officer should draft letter INT01 to the authority for signature by the intervention manager.

46. The letter will:

    (i) advise the authority it is subject to an intervention and state the level of the intervention

    (ii) explain why the SIC is making the intervention, with reference to FOI law and/or Codes of Practice, and the evidence that led to our concern

    (iii) what the intervention aims to achieve (with qualitative and quantitative targets as appropriate) or, if an assessment is required first, how this will be carried out and what it aims to establish

    (iv) the action required of the authority at this stage e.g., to conduct a self-assessment, provide a draft action plan for approval, or seek co-operation with an initial assessment

    (v) the expected timescales for the steps in the intervention

    (vi) a link to these procedures so that the authority can see what is likely to happen if the desired improvement is not achieved.

Monitoring progress

47. The method of monitoring of the intervention depends on the nature and scale of the intervention. In many cases we require a specified practice issue be resolved or a process amended. Confirmation by the authority that it has complied with the requirement will usually be sufficient for us to close the intervention.

48. In other cases, however, more complex monitoring of performance is required over time. In such cases we will generally require monthly submission of progress against the action plan e.g.,

    - Regular updates of steps taken to improve practice
    - Submission of regular performance statistics
    - Evidence of improvements, such as copies of training materials

49. The intervention officer is responsible for ensuring the authority provides satisfactory confirmation of compliance or monthly progress reports. The intervention officer must carefully examine all updates provided to ensure they comply with what the authority was asked to do.

50. If individual updates achieve a desired improvement, the intervention officer should confirm this to the authority and notify the intervention manager and named colleagues.

51. If the authority's updates are unsatisfactory, the intervention officer should communicate this to the authority, resolving any misunderstandings, agreeing a date by which the desired improvement will be achieved. If an authority appears to be resisting compliance the intervention officer should alert the intervention manager immediately. The intervention manager may recommend (internally) escalating the level of the case, or make contact with a senior manager in the authority to try to resolve the problem.

52. When the authority has achieved all of the desired improvements in the intervention, see Review.

Review

53. At the end of the monitoring period, we will evaluate whether the desired outcome has been achieved and whether the improvement is likely to be sustained.

54. The intervention manager may decide to:

    (i) Close the intervention (see Closure below)

    (ii) Close the formal intervention, but continue quarterly monitoring of practice to ensure performance is sustained

    (iii) Extend the monitoring period to allow for further improvements, or

    (iv) Escalate the intervention e.g., to a higher Level of intervention or to a practice recommendation/enforcement notice

55. The intervention officer will provide details of the outcome of the review for the monthly interventions report.

Closing an intervention

56. Closure is confirmed through a letter signed by the intervention manager. It confirms the required improvements have been made and advises of any further monitoring.

57. Before closing an intervention case file:

    (i) The case officer must ensure that all relevant information is saved within the file.

    (ii) The intervention officer must ensure that all extraneous information is securely destroyed. Particular care should be taken to destroy copies of samples of information requests provided to us for the purposes of the intervention by the authority.

58. The hard copy file should be destroyed in line with our records retention schedule.

Internal reporting

59. The intervention officer is responsible for providing:

    (i) regular progress updates to the intervention manager and their line manager (if different).

    (ii) updates for the Monthly and Quarterly Interventions Reports (due five working days before the Investigations Performance Meeting).

External reporting and publication

60. Current formal interventions are reported on the SIC website. The report is updated each month by the P&I team and provides a list of the authorities concerned, with:

    (i) the level and nature of intervention

    (ii) the basis of the intervention

    (iii) any improvement targets agreed

    (iv) the stage of each intervention (i.e. open, monitoring, closed)

61. The SIC Annual Report and Accounts provide information on the volume and types of interventions that have been undertaken and may include specific case studies.

Appendix 1: Records management

General

1. Staff must comply with the Commissioner's Information and Records Management Handbook (VC85931). The following points give some additional information specific to interventions.

2. **Information relating to an intervention must be kept safely and securely. Remember that it is a criminal offence to disclose information obtained in relation to an intervention without lawful authority.**

3. All correspondence received (or prepared) in connection with an intervention must be saved in the relevant WorkPro file as soon as possible. Accurate records of all telephone conversations and notes from meetings (bearing in mind our duties under data protection legislation) must also be added to the WorkPro file at the earliest opportunity, so that an accurate, up-to-date record of the case is maintained.

4. All drafts of letters or emails which are not used should be deleted as soon as possible.

5. Unless the case involves national security or is deemed exceptionally sensitive by HOE (when separate arrangements will be made), any paper files or document boxes used in relation to the intervention will be kept in a locked cupboard in the case manager's room. The cupboards must be kept locked at all times, except when in use.

6. Files and document boxes must never be left unattended and must be locked away when not in use.

Removing case files from the building

7. Ideally, case files should not be taken out of the office, but if there is a genuine need to do this, it must be cleared with the appropriate manager first.

8. A record of this permission, stating the period that the file has been allowed out for, must be logged in the outgoing file register (held by HOE in Inglis), at the point of removal. The return of the file must also be recorded in the register.

File security when outside the building

9. In the rare event of files being taken out of the building, it is the officer's responsibility to ensure that the files are not put at risk. The following guidance should be followed by staff:

    - Files must be returned to the office as soon as possible. Files should be taken straight home, or straight to the meeting with the public authority involved. If this is not possible, they must be locked out of sight in the boot of the car only until such time they can be returned to the office or, failing which, kept temporarily in the officer's home.

    - When carrying files in public, officers must ensure that they are concealed and well protected from the elements. Officers must never leave files unattended in public.

    - Officers must not work with files on public transport or in public areas, e.g. cafés. They may contain sensitive information and so should not be put at risk of being accessed by the general public.

Procedure for lost or stolen files

10. The Commissioner's Information and Records Management Handbook sets out the procedures for data security breaches. Staff must familiarise themselves with the Handbook. The main thing to remember is that in the event of a security breach (or a near-miss), it must be reported immediately to the FAM (in whose absence, the HOCS, whom failing another member of the SMT).

11. The appropriate manager should also be notified immediately.

12. In the event of a file going missing while it is out of the building:

- If it is lost, the responsible officer must check all places where it might have been left/stored.

- If it cannot be found after extensive searching, the officer must inform FAM and the appropriate manager immediately, who will then assess whether the file is at risk of unauthorised access, what information has been lost and what information is recoverable from scanned versions.

- If the file has been stolen, FAM and the appropriate manager must be informed immediately and will inform the local police in the area where it was stolen, if they have not been informed already. Again, FAM and the appropriate manager should also determine with the member of staff what information has been lost and what is recoverable from scanned documents.

- If an original evidence file has been lost in transit every effort must be made to locate it. If this fails, the responsible Officer must then inform FAM and the appropriate manager, who will determine if the police should be informed.

- If an original file has been stolen in transit, FAM and the appropriate manager should be informed and will contact the police in the area where it was stolen, if they have not already been informed.

- It is the responsibility of the appropriate manager to inform the public authority, as soon as possible, that the information has been lost or stolen.

Appendix 2: Examples of further research/assessment

1. On allocation, the intervention officer should carry out any further research and analysis to ensure they have a detailed understanding of the breach or failings identified. That will inform the way they approach the authority and the questions they may ask. It will also help determine whether an assessment phase is required (if not already identified/determined).

2. The depth of research and analysis is determined by the practice area; the extent and type of information we already hold; the intervention officer's understanding of the issues, etc. It may involve the authority being asked to provide information, such as carrying out a self-assessment analysis using one of the SIC toolkits. Such requests for action from the authority should ordinarily be discussed with the intervention officer's supervisor prior to a request being made.

3. Examples of further research and analysis which may be appropriate are set out below.

Example Concern 1: Failure to respond within statutory timescales

4. The intervention officer already has the statistical performance information that suggested the need for the intervention. He/she now needs to know whether there are any obvious indications of the causes of the delays, e.g. staff absence or changes, training issues, a lack of management oversight.

5. Research which may be appropriate:

   (i) Do the authority's FOI statistics (see VC82862) indicate a significant increase in requests?

   (ii) How does this authority's performance compare with that of similar authorities?

   (iii) Is there relevant background in investigation case files and decision notices?

   (iv) Do non-compliance reports suggest this is part of a wider problem?

   (v) Are SIC colleagues aware of the reasons for the problems (e.g. as a result of attendance at an FOI network meeting)?

Example Concern 2: The authority's response notices are not legally competent

6. The intervention officer needs to establish the extent of, and specify, the issues that lead to that general conclusion.

7. Research which may be appropriate:

   (i) Are errors in the authority's responses consistent (suggesting a problem with response templates) or are they different across a number of cases?

   (ii) Is the problem localised to one part of the authority (we need to focus on that part) or is it common across the authority (we need to apply the intervention authority-wide)?

   (iii) Could problems be due to insufficient knowledge, inadequate resourcing, absence of guidance or even a cultural issue within the authority?

8. Sources include DNs, non-compliance reports, and investigation case files. If there is insufficient information, it may be appropriate to obtain a sample of responses to information requests from the authority or to view its template responses. It may also involve the authority being asked to provide information, such as carrying out a self-assessment analysis

using one of the SIC toolkits. Such requests for action from the authority should ordinarily be discussed with the intervention officer's supervisor prior to a request being made.

Appendix 3: Criminal offences

62. It is a criminal offence, under section 65 of FOISA and regulation 19 of the EIRs, for a public authority, or any person employed by, or subject to the direction of the authority, to alter, deface, block, erase, destroy or conceal a record held by the authority with the intention of preventing information being disclosed in response to an information request. An information request must have been made for the information before an offence will be committed. It is not an offence to alter, etc. a record in advance of an information request being made.

63. It is possible, during an intervention, that an allegation will be made that a criminal offence has been committed. If that happens, the allegation should be brought to the attention of the HOE as soon as possible.

64. In the event that such an allegation is made during an interview, the next steps will depend on who is alleged to have committed the offence.

Allegation that a third party committed an offence

65. In the event that someone alleges that a third party has committed an offence under section 65 or regulation 19, the interviewer should tell the person making the allegation that:

    (i) what they have just said suggests that a criminal offence may have been committed under section 65 or regulation 19 in that they appear to be alleging that there has been a deliberate attempt to prevent information being disclosed in response to an information request

    (ii) if we have reason to believe there is evidence to suggest an offence may have taken place, we will refer the matter to Police Scotland

    (iii) they can either continue to tell us what happened, or might have happened, or we could come back to the allegation at a later date once we have had a chance to think about what they have told us

66. The matter can then be dropped, or discussed further, depending on the views of the interviewee.

67. The allegation must be discussed with the HOE as soon as possible.

Self-incrimination

68. If, during an interview, the interviewee suggests that they themselves committed a criminal offence under section 65 or regulation 19, the interviewer needs to caution them. It is important that the following words are used:

    "I need to stop you there. I have to advise you that, under section 65(1) of the Freedom of Information (Scotland) Act 2002 and regulation 19 of the Environmental Information (Scotland) Regulations 2004, it is a criminal offence for anyone employed by a public authority, for an officer of a public authority, or for someone who is subject to the direction of a public authority, with the intention of preventing the disclosure of the information, to alter, deface, block, erase, destroy or conceal a record held by the public authority.

    I am at the stage where I consider that an offence under section 65(1) and/or regulation 19 may have occurred and consideration may be given to reporting the matter to the police.

At this stage, I have to advise you that you are now under caution - I must inform you that you are under no obligation to answer any questions but anything that you do say, will be written down and used as evidence. Do you understand?"

69. In the unlikely event that this happens, the interviewer should end the interview immediately after the caution and bring the matter to the attention of the HOE as soon as possible.

Appendix 4: Whistleblowing

1. The Scottish Information Commissioner is a prescribed person under the Public Interest Disclosure Act for the purposes of FOISA and the EIRs. That means that any disclosure made to the Commissioner or to the Commissioner's staff will be a protected disclosure provided the disclosure is being made in good faith and provided the person making the disclosure reasonably believes that the matter relates to a breach of FOI law.

2. If, during an interview in relation to an intervention, the interviewee suggests that they are concerned that their public authority may be breaching FOISA and/or the EIRs and that they are concerned that they may be penalised in some way by telling us about what happened, the interviewer should:

   (i) remind the interviewee that the Commissioner is a prescribed person under the Public Interest Disclosure Act for the purposes of FOISA and the EIRs

   (ii) recommend that the interviewer read their employer's whistleblowing policy before continuing with the interview and contact Public Concern at Work for free advice (http://www.pcaw.org.uk/ or 020 7404 6609).

3. Whistleblowing will not necessarily happen during an interview. Any correspondence which appears to include a whistleblowing allegation, whether or not connected to an intervention, should be brought as soon as possible to the attention of the HOE.

Document control sheet

Document Information	
Full name of current version: Class, Title, Version No and Status.	C2 Intervention Procedures v03 CURRENT ISSUE
VC FileId	104657
Type	Procedure
Approver	SMT
Responsible Manager	HOPI
Date of next planned review	March 2021
Approval & Publication	
Approval Date (major version)	05/07/18
For publication *(Y/N)*	Y
Date published	05/07/18
Name of document in website file library	InterventionProcedures
Corrections / Unplanned or Ad hoc reviews (see Summary of changes below for details)	
Date of last update	

Summary of changes to document				
Date	**Action by** *(initials)*	**Version updated** *(e.g. v01.25-36)*	**New version number** *(e.g. v01.27, or 02.03)*	**Brief description** (*e.g. updated paras 1-8, updated HOPI to HOOM, reviewed whole section on PI test, whole document updated, corrected typos, reformatted to new branding*)
05/07/18	KB	03.00	03.01	New document created following approval of draft
05/07/18	KB	03.01	03.02	DCS updated, published on website

Scottish Information Commissioner
Kinburn Castle
Doubledykes Road
St Andrews, Fife
KY16 9DS

t 01334 464610
f 01334 464611
enquiries@itspublicknowledge.info

www.itspublicknowledge.info