LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

Committee: **AUDIT COMMITTEE**

Date: **WEDNESDAY, 27 NOVEMBER 2019**

Venue: **LANCASTER TOWN HALL**

Time: **6.10 P.M.**

A G E N D A

1. **Apologies for Absence**

2. **Minutes**

   Minutes of meeting held on 30 October 2019 (previously circulated).

3. **Items of Urgent Business authorised by the Chair**

4. **Declarations of Interest**

   To receive declarations by Councillors of interests in respect of items on this Agenda.

   Councillors are reminded that, in accordance with the Localism Act 2011, they are required to declare any disclosable pecuniary interests which have not already been declared in the Council's Register of Interests. (It is a criminal offence not to declare a disclosable pecuniary interest either in the Register or at the meeting.)

   Whilst not a legal requirement, in accordance with Council Procedure Rule 9 and in the interests of clarity and transparency, Councillors should declare any disclosable pecuniary interests which they have already declared in the Register, at this point in the meeting.

   In accordance with Part B Section 2 of the Code of Conduct, Councillors are required to declare the existence and nature of any other interests as defined in paragraphs 8(1) or 9(2) of the Code of Conduct.

5. **Update of the Regulation of Investigatory Powers Act 2000 (RIPA) Policy** (Pages 3 - 28)

   Report of the Information Governance Manager

6. **Internal Audit Monitoring** (Pages 29 - 47)

   Report of the Internal Audit and Assurance Manager

7. **Review of the Council's Risk Management Policy** (Pages 48 - 65)

   Report of the Internal Audit and Assurance Manager

8. **Approval of the Council's Statement of Accounts 2018/19**

Verbal update from the Council's Section 151 Officer

9. **Role of the External Auditor**

Presentation to be provided

10. **Periodic Private Discussion with External Auditor**

Discussion with the External Auditor

ADMINISTRATIVE ARRANGEMENTS

(i) Membership

Councillors Paul Stubbins (Chair), Geoff Knight (Vice-Chair), Alan Biddulph, Abbott Bryning, Jason Firth, Oliver Robinson and Malcolm Thomas

(ii) Substitute Membership

Councillors Jake Goodwin, Tricia Heath, David Whitaker, David Whitworth and Joanna Young

(iii) Queries regarding this Agenda

Please contact Sarah Moorghen, Democratic Services - telephone 01524 582132, or email smoorghen@lancaster.gov.uk.

(iv) Changes to Membership, substitutions or apologies

Please contact Democratic Support, telephone 01524 582170, or email democraticsupport@lancaster.gov.uk.

KIERAN KEANE,
CHIEF EXECUTIVE,
TOWN HALL,
DALTON SQUARE,
LANCASTER, LA1 1PJ

Published on Tuesday 19 November 2019.

AUDIT COMMITTEE

Update of the Regulation of Investigatory Powers Act 2000 (RIPA) Policy
27 November 2019

Report of, the Information Governance Manager

PURPOSE OF REPORT
To approve the proposed changes to the authority's "RIPA" policy as detailed in this report, specifically in relation to the use of Social Media and the implications that this may have.
This report is public.

RECOMMENDATIONS

(1) Members are requested to approve the revised RIPA policy attached at Appendix A to reflect the guidance contained in the revised Code of Practice for Covert Surveillance and Property Interference (August 2018)

1.0 Introduction

1.1 Local authorities can undertake surveillance and access communications data under the framework of the Regulation of Investigatory Powers Act 2000. The rules set high standards for all public authorities that use these powers to undertake a range of enforcement functions to ensure they can keep the public safe and bring criminals to justice, whilst protecting individuals' rights to privacy.

1.2 The RIPA policy was last reviewed and approved by the audit committee on 28 November 2018.

Following the revision of the Code of Practice in August 2018 and the omission in the update of November 2018, the policy has been amended to include:

1) Social Media Surveillance information,
2) The process to be followed for access to Social Media for investigation
3) Officer training.

2.0 Proposal Details

2.1 The Code of Practice requires a number of best working practices to be adopted by all public authorities, including:

- An annual review of the authority's use of RIPA to ensure that it is being used consistently and in accordance with the Council's policy; and
    - An annual review of the policy ensuring that it remains fit for purpose

2.2 In 2017 The Investigatory Powers Commissioner's Office (IPCO) took over the inspection and oversight functions on the application of RIPA, which was previously carried out by the Surveillance Commissioner's Office.

2.3 The IPCO have stated that they will continue to ensure Local Authorities are complying with RIPA by conducting a programme of inspections. As a generality, their aim is to inspect each authority once every three years but have also introduced remote desktop inspections for authorities that have significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns.

Lancaster City Council has made one RIPA authorisation since 2014 and as such when Mr Graham Wright, the IPCO inspector, completed his report of September 2017, he did so without a visit to the council.

It is not clear as to whether the council will require a desktop inspection on this occasion, but this should become clear once the IPCO has reviewed Lancaster's Annual Statistical Return.

2.4 The Council's next Annual Statistical return is due in January 2020.

2.5 This committee will be asked to complete the annual review of the authorities use of RIPA in their February 2020 meeting.

2.6 The Information Governance Manager will ensure that staff requiring guidance on the use and application of RIPA are provided with training or refresher training (including the use of social media) whichever is appropriate to ensure that the council remains compliant with the law.

3.0 Details of Consultation

3.1 The Monitoring Officer, Legal Services and Corporate Fraud have been consulted in compiling this report.

4.0 Options and Options Analysis (including risk assessment)

4.1 There are no other options available. It is necessary to carry out a regular review and update of the RIPA policy to ensure it supports the council's officers and protects the rights of the public when carrying out surveillance.

If there is no clear guidance on the use of social media, the council is at risk of falling foul of the law when attempting to go about its business which simply cannot be risked.

5.0 Conclusion

5.1 Updating the policy will ensure that the council remains compliant with the law and will ensure that Officers are able to provide auditable records of activity in relation to social media.

CONCLUSION OF IMPACT ASSESSMENT **(including Health & Safety, Equality & Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing):** Not Applicable
LEGAL IMPLICATIONS The approval of this recommendation will ensure that the statutory requirements are complied with.
FINANCIAL IMPLICATIONS None directly arising from this report. Training for staff to ensure that they are kept up to date with appropriate practice and revisions to RIPA will be allocated from existing budgets.
SECTION 151 OFFICER'S COMMENTS The Section 151 Officer has been consulted and has no further comments.
MONITORING OFFICER'S COMMENTS The Monitoring Officer has been consulted and has no further comments.

BACKGROUND PAPERS None	**Contact Officer:** Amy Holland **Telephone:** 01524 58 2205 **Email:** ajholland@lancaster.gov.uk

LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY AND PROCEDURE

Document Control

Approved by:	Audit Committee	**Date:**	28/11/2018
Document location:			
Document owner:	Information Governance		
Review period:	2 Years		
Next review date:	28/11/2020		

Revision History

Version	Date	Reviewed By	Amendment Details
V 1.0	28/11/2018	Audit Committee	Approval of final draft
V1.1	06/11/2019	A Holland	Social Media Use and guidance

CONTENTS

1 Purpose 5
2 Introduction 5
3 Office of the Surveillance Commissioner 7
4 Statement of Intent 7
5 Part 1: An explanation of the Key Provisions of RIPA 7
5.1 What is meant by 'surveillance'? 7
5.2 When is surveillance "covert"? 7
5.3 What is 'directed surveillance' or when is surveillance 'directed'? 7
5.4 Is it for the purposes of a specific investigation or operation? 8
5.5 Is it in such a manner that it is likely to result in the obtaining of private information about a person? 8
5.6 What is meant by 'intrusive surveillance' or when is surveillance 'intrusive'? 8
5.7 Why is it important to distinguish between directed and intrusive surveillance? 9
5.8 What is a 'covert human intelligence source' (CHIS)? 9
5.9 Use of Social Networking in investigations 10
6 Part 2: General Authorisation Requirements 11
6.1 The authorisation requirements 11
6.2 Who can authorize the use of covert surveillance? 12
6.3 Justification for covert surveillance 12
6.4 CHIS – additional requirements 13
6.5 Collateral Intrusion 13
6.6 Local community sensitivities 14
7 Part 3: Directed Surveillance Authorisation Requirements 14
7.1 Applications for directed surveillance authorisation 14
7.2 Duration of directed surveillance authorisations 14
7.3 Reviews of directed surveillance authorisations 14
7.4 Renewals of directed surveillance authorisations 14
7.5 Cancellation of directed surveillance authorisations 14
7.6 Ceasing of surveillance activity 15
7.7 Urgent Cases 15
7.8 Confidential Information 15
8 Part 4: CHIS Authorisation Requirements 16
8.1 Duration of CHIS authorisations 16
8.2 Renewal of CHIS Authorisations 16
8.3 CHIS Forms 16
8.4 Vulnerable Adults 16
8.5 Juvenile Sources 16
9 Part 5: Other Authorisation Requirements 17
9.1 Retention and destruction of the product of surveillance 17
9.2 Acting on behalf of another 18
10 Part 6: Practical Application of RPIA 18
10.1 Who is affected by RIPA? 18
10.2 'General observation vs. 'systematic surveillance' 18
10.3 'Covert' vs. 'overt' surveillance 18
10.4 CCTV 19
10.5 Recognising a CHIS 19
10.6 "…. establishing or maintaining a personal or other relationship……" 19
10.7 Simple test purchase transactions 20
10.8 Use of DAT recorders 20
10.9 RIPA forms 20
10.10 Role of Authoring Officers 20
10.11 How to access RIPA documents? 21

11 Training and awareness 21
Appendix 1: 22
Appendix 2: 23

1 Purpose

The purpose of this policy is to:

- explain the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA);
- provide guidance and give advice to those Services undertaking covert surveillance; and
- ensure full compliance with RIPA and a Council-wide consistent approach to its interpretation and application.

2 Introduction

RIPA came into force on 25th September 2000 to regulate covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

Lancaster City Council is therefore included within the 2000 Act framework with regard to the authorisation of both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS)

In summary RIPA requires that when a Council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. In addition, amendments contained in the Protection of Freedoms Act 2012, which took effect on the 1st November 2012, mean that local authority authorisations, and renewals of authorisations under RIPA, can only take effect once an order approving the authorization (or renewal) has been granted by a Justice of the Peace (district judge or lay magistrate) (JP).

Authorisation for both types of surveillance may be granted only where it is believed that the authorisation is necessary, and the authorised surveillance is proportionate to that which is sought to be achieved:

An authorisation may be granted only where the Authorising Officer believes that the authorisation is necessary in the circumstances of the particular case:

"For the purpose of preventing and detecting crime and disorder"

However, amendments which took effect on the 1st November 2012 mean that a local authority may only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least 6 months' imprisonment. These amendments are referred to as "the crime threshold".

The background to RIPA is the Human Rights Act 1998, which imposes a legal duty on public authorities to act compatibly with the European Convention on Human Rights (ECHR). Article 8(1) of the ECHR gives a right to respect for private and family life, the home and correspondence. However, this is qualified by Article 8(2) which provides that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national

security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. RIPA was enacted so as to incorporate the provisions of Article 8(2) in English law, and to establish a means by which a public authority may interfere with privacy rights in accordance with the law. The objective is to give protection to the Council and any officer involved in an investigation. The scheme of RIPA is to state that an authorisation for covert surveillance shall be lawful for all purposes, but that such an authorisation may only be granted if the authorising officer believes that what is proposed is necessary and proportionate (see paragraphs 35 and 36 below).

If the authorisation procedures introduced by RIPA are followed, they afford protection to the Council and to investigating officers in respect of challenges to the admissibility of evidence, claims under the Human Rights Act 1998, and complaints to the Local Government Ombudsman or the Investigatory Powers Tribunal.

The Act is supported by statutory Codes of Practice, the most recent versions of which were published in 2014 and are available on the Council's intranet. These are the 'Covert Surveillance and Property Interference' Code of Practice and the 'Covert Human Intelligence Sources' (CHIS) Code of Practice. RIPA requires the Council to have regard to the provisions of the Codes which are admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal. However, amendments which took effect on the 1st November 2012 mean that a local authority may only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment or are related to the underage sale of alcohol and tobacco. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence punishable by a maximum term of at least 6 months' imprisonment. These amendments are referred to as "the crime threshold".

The background to RIPA is the Human Rights Act 1998, which imposes a legal duty on public authorities to act compatibly with the European Convention on Human Rights (ECHR). Article 8(1) of the ECHR gives a right to respect for private and family life, the home and correspondence. However, this is qualified by Article 8(2) which provides that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. RIPA was enacted so as to incorporate the provisions of Article 8(2) in English law, and to establish a means by which a public authority may interfere with privacy rights in accordance with the law. The objective is to give protection to the Council and any officer involved in an investigation. The scheme of RIPA is to state that an authorisation for covert surveillance shall be lawful for all purposes, but that such an authorisation may only be granted if the authorising officer believes that what is proposed is necessary and proportionate (see paragraphs 35 and 36 below).

If the authorisation procedures introduced by RIPA are followed, they afford protection to the Council and to investigating officers in respect of challenges to the admissibility of evidence, claims under the Human Rights Act 1998, and complaints to the Local Government Ombudsman or the Investigatory Powers Tribunal.

The Act is supported by statutory Codes of Practice, the most recent versions of which were published in 2014 and are available on the Council's intranet. These are the 'Covert Surveillance and Property Interference' Code of Practice and the 'Covert Human Intelligence

Sources' (CHIS) Code of Practice. RIPA requires the Council to have regard to the provisions of the Codes which are admissible as evidence in criminal and civil proceedings and must be taken into account by any court or tribunal.

3 Office of the Surveillance Commissioner

In May 2001 an Inspectorate was formed within the Office of Surveillance Commissioners (OSC) to assist the 'Chief Surveillance Commissioner' keep under review the exercise and performance of the powers and duties conferred or imposed by RIPA. The most recent Procedures and Guidance document was issued by the Chief Surveillance Commissioner in December
2014, and is available on the Council's intranet.

RIPA requires public authorities to disclose or provide to the Chief Surveillance Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions.

4 Statement of Intent

The Council's policy and practice in respect of RIPA is to comply fully with the law and strike a fair and proportionate balance between the need to carry out covert surveillance in the public interest and the protection of an individual's fundamental right to privacy. The Council acknowledges that this policy is very much a living document and will be reviewed and updated in line with the best guidance and advice current at the time.

5 Part 1: An explanation of the Key Provisions of RIPA

5.1 What is meant by 'surveillance'?

'Surveillance' includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

5.2 When is surveillance "covert"?

According to RIPA, surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the 2000 Act framework does not apply.

5.3 What is 'directed surveillance' or when is surveillance 'directed'?

Surveillance is directed if it is 'covert' but not 'intrusive' (see below) and is undertaken:

a) for the purposes of a specific investigation or a specific operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not that person is specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Essentially, therefore, directed surveillance is any:

(1) pre-planned surveillance activity;
(2) undertaken covertly;
(3) for the purposes of a specific investigation;
(4) in such a way that is likely to result in obtaining private information about a person.

5.4 Is it for the purposes of a specific investigation or operation?

For example, are CCTV cameras which are readily visible to anyone walking around a Council car park covered?
The answer is no if their usage is to monitor the general activities of what is happening in the car park. If that usage changes at any time the 2000 Act may apply.
For example, if the CCTV cameras are targeting a particular known individual, and are being used in monitoring his activities, that has turned into a specific
operation which will require authorisation.

5.5 Is it in such a manner that it is likely to result in the obtaining of private information about a person?

5.5.1 'Private Information'

In relation to a person, includes any information relating to his private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration.

If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the 2000 Act framework. However, the use of "test purchasers" may involve the use of covert human intelligence sources see section 10.7

5.5.2 'Immediate response…'

According to the Covert Surveillance Code of Practice, "covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under the 2000 Act would not require a directed surveillance authorisation." For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

However, if as a result of an immediate response, a specific investigation subsequently takes place, that brings it within the 2000 Act framework.

5.6 What is meant by 'intrusive surveillance' or when is surveillance 'intrusive'?

Surveillance becomes intrusive if the covert surveillance:

a) is carried out in relation to anything taking place on any 'residential premises' or in any 'private vehicle'; or a "place for legal consultation; and

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device; or

c) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, and the device is such that it **consistently provides information of the same quality and detail** as might be expected to be obtained from a device actually present on the premises or in the vehicle.

The definition of surveillance as intrusive relates to the location of the surveillance, and not to other consideration of the nature of the information that is expected to be obtained. Officers of the Council are unlikely to have access to any "place of legal consultation" but should seek advice from Legal Services on the detailed definition.

5.6.1 'Residential premises'

Is defined to include any premises that is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. For example, the definition includes hotel rooms. It, however, does not include so much of any premises as constitutes any common area to which a person is allowed access in connection with his use or occupation of any accommodation. For example, a hotel lounge.

5.6.2 'Private vehicle'

Means any vehicle which is used primarily for private purposes, for example, for family, leisure or domestic purposes. It therefore does not include taxis i.e. private hire or hackney carriage vehicles.

5.7 Why is it important to distinguish between directed and intrusive surveillance?

It is imperative that officers understand the limits of directed surveillance or, put another way, recognise when directed surveillance becomes intrusive surveillance because **RIPA does not permit local authorities to undertake intrusive surveillance in any circumstances.**

5.8 What is a 'covert human intelligence source' (CHIS)?

According to RIPA a person is a CHIS if:

a) he **establishes or maintains a personal or other relationship** with a person for the **covert purpose** of facilitating the doing of anything falling within paragraph b) or c).

b) he covertly uses such a relationship to **obtain information** or provide access to any information to another person; or

c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A CHIS is effectively an inside informant or undercover officer, someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator.

A **purpose is covert**, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

It is not clear whether **'information'** is restricted to private information in line with directed surveillance. The inference is there, but it is not clear. If in doubt, the Council's policy is to obtain an authorisation.

RIPA also makes reference to the use of a CHIS which refers to inducing, asking or assisting a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of such a CHIS.

5.9 Use of Social Networking in investigations

Officers often use the internet and social networking sites for the purposes of research and carrying out checks on the subjects of an investigation. Care must be taken to ensure that officers do not stray into a surveillance situation.

It should not be assumed that all monitoring of open social media sites are automatically immune from the need for an authorisation of some sort. Use of open media, in circumstances where there is a reasonable expectation of privacy, is likely to require an authorisation, particularly if the monitoring is intensive or for a prolonged period of time i.e. more than a week. The creation of fake or anonymous websites for investigation purposes is likely to require an authorisation. Entry on to chat rooms or closed groups for investigatory purposes is also likely to require authorisation unless the officer's identity is made clear from the outset.

Use of a 3rd party's identity requires both an authorisation and express written permission from that person. Whilst overt working in this way might avert the need for a surveillance authorisation officers should be aware that a CHIS situation could inadvertently arise.

It is expected that social media sites will generate significant amounts of sensitive information.

Sensitive material that is not relevant to an investigation should be disposed of quickly and safely. Any interaction between an investigator and the public via social media could inadvertently give rise to a CHIS situation. Investigators should generally avoid interaction whilst monitoring social media sites and take advice should any uncertainty arise. The use of the internet and social media may require an authorisation in the following circumstances:

(a). Any communications which are made with 3rd parties for the purpose of gathering evidence or intelligence about an offence in circumstances where the third party is not aware that the officer is working for the Council.

(b) Accessing private pages of social media for the purpose of gathering evidence or intelligence about an offence or other matter subject to potential litigation.

(c). Any communications between an officer and a 3rd party for the purpose of using that person to gather evidence or intelligence about a suspect.

(d). Intensive monitoring of a suspect using social media over a sustained period of time particularly when this is used in connection with other methods of investigation.

(e). The creation of a false personae or use of a third-party identity for investigation purposes.

(f). Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, when they are not explicit about their real identity.

Repeated entry to social media sites and copying material for the purpose of an investigation is likely to engage RIPA. As a rule of thumb access to Facebook and other social media sites should be made via the Council's Facebook account as opposed to a private account. If there is any doubt the officer who is conducting this activity is advised to seek legal advice.

Please see **Appendix 2** for the process which is to be followed in relation to the use of social media.

The OSC has issued the following guidance: -

- Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases, data may be deemed private communication still in transmission (instant message for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

- Providing there is no warrant authorising interception in accordance with section 48 (4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than the mere reading of the site's content).

- It is not unlawful for a member of a public authority to set up a false identity, but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity potentially infringes other laws.

- A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done.

6 Part 2: General Authorisation Requirements

6.1 The authorisation requirements

RIPA requires that prior authorisation is obtained by all local authorities using directed surveillance and CHIS techniques.

The authorising officer must give authorisations in writing and a separate authorisation is required for each investigation. Any authorisation must also be approved by an order from a JP. The application form for such approval is available on the Council's intranet, but advice should be sought from Legal Services on making an application for judicial approval.

Whilst according to RIPA, a single authorisation may combine two or more different authorisations (for example, directed surveillance and CHIS), the provisions applicable in the case of each of the authorisations must be considered separately. Because combining authorisations may cause confusion, officers must use separate forms for different authorisations.

The purpose of the authorisation is to comply with the Human Rights Act 1998 by providing lawful authority to carry out surveillance. This is why an authorisation must be obtained where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. If the surveillance is then actually carried out in accordance with the authorisation, it will be less open to challenge.

6.2 Who can authorize the use of covert surveillance?

To give effect to RIPA, The Director of Corporate Services has been designated to authorise the use of directed surveillance and CHIS techniques in respect of external investigations and to sanction the use of such covert surveillance in respect of internal officer/Member investigations. This designation can be directly delegated to the Monitoring Officer Any RIPA authorisation must be approved by an order from a JP. The JP will be provided with a copy of the authorisation, and with a partially completed judicial application/order form, which is available on the Council's intranet. Advice should be sought from Legal Services, who will contact the court to arrange the hearing date for the application.

It should also be noted that in accordance with the relevant Regulations, the designation of the Director of Corporate Services to sanction the use of RIPA regulated covert surveillance extends upwards to the Chief Executive.

Ideally, the Authorising Officer should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, the Codes of Practice recognize that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently.

6.3 Justification for covert surveillance

In order to use covert surveillance (both directed surveillance and a CHIS) lawfully the person granting the authorisation (i.e. the authorising officer) will have to demonstrate that the surveillance is both 'necessary' and 'proportionate' to meet the objective of the prevention or detection of crime or of prevention of disorder. The JP must also be satisfied that the use of the technique is necessary and proportionate.

6.3.1 The 'necessity' test

RIPA first requires that the authorising officer must be satisfied that the authorisation is necessary, in the circumstances of the particular case, for the prevention and detection of crime, or prevention of disorder. This is the only statutory ground on which local authorities are now able to carry out directed surveillance and use a CHIS. For the purposes of the authorisation of directed surveillance, the crime threshold referred to in paragraph 4 above must be met. Covert surveillance cannot be "necessary" unless, in that particular case, there is no reasonably available overt method of discovering the desired information.

6.3.2 The 'proportionality' test

Then, if the activities are necessary, the authorising officer must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is **excessive** in the circumstances of the case or if the information which is sought could reasonably be obtained **by other less intrusive means**. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

6.4 CHIS – additional requirements

In addition, there are further criteria in relation to CHIS authorisations. Namely, that specific arrangements exist to ensure that, amongst other things, the source is independently managed and supervised, that records are kept of the use made of the source, that the source's identity is protected from those who do not need to know it, and that arrangements also exist to satisfy such other requirements as may be imposed by an Order made by the Secretary of State.

RIPA provides that an authorising officer must not grant an authorisation for the use or conduct of a source unless he believes that arrangements exist that satisfy these requirements. In this regard, the particular attention of authorising officers is drawn to paragraph 6.14 of the CHIS Code of Practice concerning the security and welfare of a CHIS and the need to carry out a **risk assessment**.

The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI No. 2725) details the particulars that must be included in the records relating to each CHIS. The authorising officer should comment on all these aspects in his "comments" box, as he may have to justify the fact that he has taken account of these requirements and made an appropriate provision to comply.

6.5 Collateral Intrusion

Before authorising surveillance, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (particularly when considering the proportionality of the surveillance). This is referred to as collateral inclusion, and the following should be considered:

I. measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those not directly connected with the investigation or operation;

II. an application for an authorisation should include an assessment of the risk of any collateral intrusion and the authorising officer should take this into account, when considering the proportionality of the surveillance;

III. those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation; and

IV. when the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.

6.6 Local community sensitivities

Any person applying for or granting an authorisation will also need to be aware of what the Codes of Practice refer to as “any particular sensitivities in the local community” where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

7 Part 3: Directed Surveillance Authorisation Requirements

7.1 Applications for directed surveillance authorisation

Applications for authorisation to carry out directed surveillance must be made in **writing** using the **standard Application Form** and judicial approval form available on the Council’s intranet.

7.2 Duration of directed surveillance authorisations

A written authorisation granted by an authorising officer, and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

7.3 Reviews of directed surveillance authorisations

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to **‘confidential information’** (see below) or involves collateral intrusion.

Authorisations must be reviewed by the authorising officer therefore **at least monthly** using the **standard Review Form** available on the Council’s intranet to ensure that they remain in force only for so long as it is necessary.

7.4 Renewals of directed surveillance authorisations

If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for **a further period of three months** using the **standard Renewal Form** available on the Council’s intranet. The same conditions attach to a renewal of surveillance as to the original authorisation. An order from a JP is required for a renewal in the same way as for an authorisation.

A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until **10 working days** before the authorisation period is drawing to an end. However, where renewals are timetabled to fall outside of court hours, for example during a holiday period, care must be taken to ensure that the renewal is completed ahead of the deadline.

Any person who would be entitled to grant a new authorisation can renew an authorisation, but an order from a JP is also required. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

7.5 Cancellation of directed surveillance authorisations

The authorising officer who granted or last renewed the authorisation **must** cancel it using the **standard Cancellation Form** available on the Council’s intranet if he is satisfied that the

directed surveillance no longer meets the criteria upon which it was authorised. Authorisations should not be allowed to simply expire.

Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer or the person who is acting as authorising officer **(see the Regulation of Investigatory Powers (Cancellation of Authorisations) Order 2000; SI No: 2794).**

If the authorising officer is on sick or annual leave or is otherwise unable to cancel the authorisation for good reason, any other officer designated to grant authorisations may cancel the authorisation.

7.6 Ceasing of surveillance activity

As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the notification of cancellation where relevant (see standard cancellation form).

7.7 Urgent Cases

A JP may consider an authorisation out of working hours in exceptional cases. This must be arranged through the court, and two completed judicial application/order forms must be provided so that one can be retained by the JP.

7.8 Confidential Information

RIPA does not provide any special protection for 'confidential information'.
The Codes of Practice, however, do provide additional safeguards for such information. Confidential information consists of matters subject to legal privilege; confidential personal information (information relating to the physical or mental health or spiritual counselling of a person who can be identified from it) or confidential constituent information (relating to communications between a Member of Parliament and a constituent in respect of constituency matters) or confidential journalistic material (material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence). Further details about these categories of confidential information are set out in the Codes themselves, and advice can be obtained from Legal Services.

Special care should be taken if there is a likelihood of acquiring any confidential information. Such authorisations should only be granted in exceptional and compelling circumstances with full regard to the proportionality issues such surveillance raises.

In accordance with the provisions of the Code, in cases where through the use of the surveillance it is likely that confidential information will be acquired, the use of surveillance must be authorised by the Chief Executive.

If, exceptionally, any Council investigation is likely to result in the acquisition of confidential material, officers are required to obtain the prior approval of Legal Services before applying for an authorisation.

If confidential material is acquired during the course of an investigation, the following general principles apply:

- confidential material should not be retained or copied unless it is necessary for a lawful purpose;
- confidential material should be disseminated only where an officer (having sought advice from the Legal Services Manager) is satisfied that it is necessary for a lawful purpose;
- the retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information; and confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

8 Part 4: CHIS Authorisation Requirements

Generally speaking, the authorisation requirements for directed surveillance also apply to a CHIS authorisation. There are, however, some variations, and the crime threshold as set out in paragraph 4 does not apply to a CHIS authorisation.

8.1 Duration of CHIS authorisations

A written CHIS authorisation granted by an authorising officer and approved by a JP, will cease to have effect (unless renewed) at the end of a period of **twelve months** beginning with the day on which it took effect.

8.2 Renewal of CHIS Authorisations

An authorising officer may renew a CHIS authorisation in writing **for a further period of twelve months**. This is subject to approval from a JP.

The same conditions attach to a renewal of surveillance as to the original authorisation. However, before renewing an authorisation for the use or conduct of a CHIS, officers are required to carry out a review of the use made of that source, the tasks given to that source and the information so obtained.

8.3 CHIS Forms

Standard **CHIS Application; Review; Renewal, and Cancellation Forms**, and the **Judicial Approval form** are available on the Council's intranet. Officers are required to use these forms in the appropriate circumstances.

8.4 Vulnerable Adults

In accordance with the CHIS Code of Practice, a **'vulnerable perso**n' should only be authorised to act as a CHIS in the most exceptional circumstances and must be authorised by the **Chief Executive**. Legal advice should always be sought. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

8.5 Juvenile Sources

Special safeguards also apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. Legal advice should always be sought. On no occasion should the use or

conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions contained within **The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793)** are satisfied. Authorisations for juvenile sources must be authorised by the **Chief Executive** the duration of such an authorisation is **one month only** instead of the usual twelve months.

9 Part 5: Other Authorisation Requirements

The Codes of Practice provide that a centrally retrievable record of all authorisations should be held by each public authority and regularly updated whenever an authorisation is granted, reviewed, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners (OSC), upon request. These records will be retained for a period of at least three years from the ending of the authorisation and will comprise of the information prescribed in the Codes.

The Council will also maintain a record of specified documentation relating to authorisations as further required by the Codes.

To give effect to these requirements The Authorising Officer is required to e-mail all completed RIPA forms to the Monitoring Officer within two working days of the grant; review; renewal; or cancellation of the authorisation so that the Council's central recording and monitoring systems can be kept up to date.

The Authorising Officer should however ensure that original RIPA forms are kept on the investigation case file and stored securely.

In addition, the Monitoring Officer will report periodically to Audit Committee with the register of authorisations to enable them to be satisfied that RIPA authorisation requirements are being complied with.

9.1 Retention and destruction of the product of surveillance

Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review.

The Codes of Practice draw particular attention to the requirements of the code of practice issued under the **Criminal Procedure and Investigations Act 1996**. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

Where material is obtained by surveillance, which is **wholly unrelated** to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be **destroyed immediately**. Consideration of whether or not unrelated material should be destroyed is the responsibility of the authorising officer.

There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Each Service must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements relating to the handling and storage of material.

9.2 Acting on behalf of another

In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by the Police with the use of the Council's CCTV systems, an authorisation must be obtained by the Police.

10 Part 6: Practical Application of RPIA

10.1 Who is affected by RIPA?

As the Council has already recognised in respect of the application of the **Human Rights Act 1998**, RIPA will impact on the enforcement activities of all the Council's regulatory Services, but, in the case of authorisations for directed surveillance, the crime threshold referred to in paragraph 4 must be met. This means that directed surveillance will no longer be able to be used in some investigations where it was previously authorised, e.g. dog fouling. However, this does not mean that it will not be possible to investigate these matters with a view to stopping offending behaviour. Routine patrols, observation at trouble "hotspots", immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

A public authority may only engage RIPA when in performance of its "core functions" in contrast to the "ordinary functions" which are undertaken by all authorities (e.g. employment and contractual matters). Accordingly, the disciplining of an employee is not a core function, although related criminal investigations may be.

10.2 'General observation vs. 'systematic surveillance'

According to the Covert Surveillance Code of Practice "General observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act". For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder or trading standards or HM Customs and Excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

The clear view expressed therefore is that usually low-level activity such as general observation will not be regulated under the provisions of RIPA provided it does not involve the systematic surveillance of an individual. That said, the determination of what constitutes 'general observation' on the one hand and 'systematic surveillance' on the other is a question of fact, the determination of which is not always straightforward and depends on the particular circumstances of an individual case.

In practice, the issue will turn on whether the covert surveillance is likely to result in obtaining any information in relation to a person's private or family life, whether or not that person is the target of the investigation or operation. If in doubt you are strongly recommended to obtain an authorisation.

10.3 'Covert' vs. 'overt' surveillance

In accordance with the Council's usual practice, wherever possible and appropriate Services should give advance warning of their intention to carry out surveillance. This is because the

provisions of RIPA regulate the use of covert surveillance only. In some cases, a written warning may itself serve to prevent the wrongdoing complained of.

However, in order to properly put a person on notice that he is or may be the subject of surveillance, the notification letter must be couched in sufficiently precise terms so that he knows what **form** the surveillance will take (i.e. record of noise; photographs etc.). In fact, in line with directed surveillance requirements, notification letters should state **how long** the surveillance is likely to last (which should not be longer than three months); the necessity for the surveillance should be **reviewed at least monthly**; if it is necessary to continue the surveillance beyond the initial specified period a **renewal letter** should be sent to the 'noisy' neighbour, for example, and he should be informed when the surveillance has ceased.

It is also important to instruct the investigating officer not to exceed the limits of the 'surveillance' he has been asked to carry out.

Whilst it is accepted that the definition of 'covert' set out in RIPA could be interpreted very broadly, it is suggested that whether the surveillance activity is covert or not depends on the investigator's intention and conduct. If there is some element of **secrecy** or **concealment** the activity is likely to be covert.

Wherever possible or appropriate, officers should be **open; obvious and overt**.

10.4 CCTV

Overt CCTV systems used for general purposes are not usually regulated by RIPA (but CCTV in general is regulated by the Data Protection Act 2018, the GDPR 2016/679 and the CCTV Code of Practice issued by the Office of the Information Commissioner). If, however, CCTV systems are used to **track individuals** or **specific locations** and the surveillance is **pre-planned** (i.e. not an immediate response to events or circumstances which by their very nature, could not have been foreseen) **a directed surveillance** authorisation must be obtained.

10.5 Recognising a CHIS

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crime stoppers, Customs Confidential, the Anti-Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

However, when an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining the information in the course of a family or neighbourhood relationship, this probably means that the informant is a CHIS, to whom a duty of care is owed if the information is then used, even though he or she has not been tasked by the authority to obtain information on its behalf.

The use of professional witnesses to obtain information and evidence is clearly covered.

10.6 "…. establishing or maintaining a personal or other relationship……"

Whilst the meaning of "...establishing or maintaining a personal or other relationship…" is not clear and is open to interpretation, it is suggested that there has to be some measure of **intimacy** beyond the ordinary conversation. Only if an officer, for example, establishes some

measure of **trust and confidence** with the person who is the subject of the surveillance will he be establishing or maintaining a personal or other relationship.

Usually a simple enquiry or a request for general information (i.e. a request for information which would be supplied to any member of the public who enquired) not obtained under false pretences is not likely to be regulated by RIPA.

10.7 Simple test purchase transactions

Whether or not test purchase transactions are regulated by RIPA depends on the circumstances and in particular the conduct of the person carrying out the surveillance. Usually simple covert test purchase transactions carried out under existing statutory powers where the officer involved does not establish a personal or other relationship will not require a CHIS authorisation.

Officers should, however, be wary of the law on **'entrapment'**. Whereas officers can in appropriate circumstances, present a seller or supplier, for example, an opportunity which he could act upon, officers cannot 'incite' the commission of an offence i.e. encourage, persuade or pressurise someone to commit an offence.

10.8 Use of DAT recorders

If it is appropriate to do so, Environmental Health officers, and to a much lesser extent Council Housing officers, use a recorder to monitor noise levels (usually at residential premises) following noise nuisance complaints. Whilst the recorder is installed by officers, the complainant decides when to switch the recorder on and off.

The covert recording of suspected noise nuisance where the intention is only to record excessive noise levels from adjoining premises, and the recording device is calibrated to record only excessive noise levels, may not require an authorisation, as the perpetrator would normally be regarded as having forfeited any claim to privacy.

That said, a Digital Audio Tape (DAT) recorder is a sophisticated piece of monitoring equipment and if used covertly may constitute directed surveillance. In general, a letter is sent to the person who is to be the subject of the surveillance, and this should mean that subsequent surveillance is overt, and an authorisation will not as a matter of course be required. However, if there is any doubt as to whether surveillance is covert, e.g. if any longer than a few weeks has passed since the alleged perpetrator was informed that monitoring might be carried out, and if it is likely that private information will be obtained, then an authorisation should be sought.

10.9 RIPA forms

It is imperative that RIPA forms are completed in full whenever RIPA regulated surveillance activity is planned. The information given must be specific and detailed; must relate to the particular facts of an individual case (i.e. avoid standard wording if at all possible) and must demonstrate that a proper risk assessment has been carried out. Both those who apply for an authorisation and the Authorising Officer should refer to this policy and to the relevant Code of Practice in completing the relevant form,

10.10 Role of Authoring Officers

The Authorising Officer is required to ask themselves: “Have I got sufficient information to make an informed decision as to whether or not to authorise surveillance activity on the particular facts of this case?” and must recognise that RIPA imposes new and important obligations on those Services affected by RIPA

Authorising officers must be satisfied that there are adequate checks in place to ensure that the surveillance carried out is in line with what has been authorised. Such monitoring should be properly documented as well as the decision-making process in general.

Officers are strongly recommended to read this policy in conjunction with the Covert Surveillance and CHIS Codes of Practice which provide supplementary guidance.

If the surveillance is not properly authorised, the protection offered by RIPA will be lost.

10.11 How to access RIPA documents?

RIPA itself; explanatory notes to RIPA, the Covert Surveillance and CHIS Codes of Practice; RIPA statutory instruments and other RIPA documents are available on the Home Office web-site: https://www.gov.uk/government/collections/ripa-codes
Relevant RIPA documents as well as this policy and the Council’s standard forms have also been posted on the Council’s intranet.

11 Training and awareness

It is the policy of the Council to provide adequate training for all its employees so that they are aware of the RIPA provisions and know when certain activities are required to be authorised. Authorising Officers will be trained in the proper use of their powers as with investigating officers The Council seeks to ensure that all staff likely to be engaged in surveillance work and the use of CHIS understand the regulatory framework and know which officers are authorised Investigating Officers and the Authorising Officer

Training and refresher training shall be provided on a regular basis.

Appendix 1:

Directed surveillance forms

Application for the authorisation of directed surveillance:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAA0ADkAOAAzAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Review of directed surveillance authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANQAyAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Renewal of directed surveillance authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANQAzAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Cancellation of a directed surveillance authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANQA0AHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

CHIS (Covert Human Intelligence Source) forms

Application for authorisation of use or conduct of a CHIS:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAA0ADkAOAA0AHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Review of a CHIS authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANgAwAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Renewal of a CHIS authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANgAxAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Cancellation of a CHIS authorisation:
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAAyADQANgAyAHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Judicial Approval Form
http://intranet.lancaster.gov.uk/GetAsset.aspx?id=fAA0ADAAOQA5AHwAfABGAGEAbABzAGUAfAB8ADAAfAA1

Appendix 2:

PROCESS TO BE FOLLOWED WHEN CONSIDERING USING SOCIAL NETWORKING SITES IN INVESTIGATIONS OR TO GATHER EVIDENCE.

Where an officer considers it necessary to view a social networking site to investigate an allegation or to gather information the following process is to be followed:

1. Officers must not use their own personal or private account when accessing social networking sites for investigations/evidence gathering, only Council accounts should be used.

2. Officers may access the main page of an individual's profile to take an initial view as to whether there is any substance to the allegation of the matter being investigated and is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation.

3. Officers are required to keep a log recording when social networking sites are viewed for investigations/evidence gathering. Each viewing of a company or individual's social networking site must be recorded on the log. This is to enable the Council to monitor the use of these sites for investigations/evidence gathering and use this information to review policies and guidance.

4. If it is considered that there is a need to monitor a company's or individual's social networking site, for example by systematically collecting and recording information about a particular person or group, then the officer must refer the matter to their Head of Service for consideration as to whether a RIPA authorisation from the Magistrates Court may be required. If officers are in any doubt as to whether an authorisation is required, they should seek advice from the Information Governance Manager or Authorising Officer (Director for Corporate Services), before continuing to access a social networking site.

5. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by the Council's Authorising Officer and then approved by a Magistrate.

6. If the offence being investigated falls outside RIPA, a 'Non-RIPA' form must be completed and forwarded to the Authorising Officer.

7. Officers also need to be aware that any evidence captured as part of a criminal investigation will need to comply with the relevant legislation (The Police and Criminal Evidence Act 1984, Criminal Procedure Rules 2018 and the Criminal Procedure and Investigations Act 1996) and advice should be sought from the Council's Legal Services Manager.

8. A copy of all forms should be forwarded to the Council's Information Governance Manager so that a central record of RIPA requests and Authorisations can be kept.

AUDIT COMMITTEE

Internal Audit Monitoring
27 November 2019

Report of Internal Audit and Assurance Manager

PURPOSE OF REPORT
To advise Members of the latest monitoring position regarding the 2019/20 Internal Audit plan. To advise Members of the latest monitoring position regarding the implementation of the Annual Governance Statement (AGS) action plan for 2018/19.
This report is public

RECOMMENDATIONS

(1) That the latest monitoring position in relation to the audit plan be noted.

(2) That the last progress in relation to the AGS action plan for 2018/19 be noted.

1.0 Audit Plan monitoring to 1 November 2019

1.1 The 2019/20 Internal Audit plan was approved by the Audit Committee at its meeting on 20 February 2019. This report is based on the monitoring position up to 1 November 2019.

1.2 **Summary of monitoring position at 1 November 2019**

	Report Status				
Category of Audit	**Final Report Issued**	**Assurance Level**	**Fieldwork**	**Draft Report Issued**	**Comments**
Carried forward 2018/19 audit work					
Financial Planning and Medium Term Financial Statement (MTFS			✓		Due to be completed by Lancashire County Council
Recovery of Legal Fees and Court Costs					Will be completed in Q4
Council Housing Assets			✓		To start January 2020
Economic Development / Regeneration Strategy					Will be completed in Q4
Insurance	Final Report Issued October 2019	Limited			Post audit review due January 2020

	Report Status				
Category of Audit	**Final Report Issued**	**Assurance Level**	**Fieldwork**	**Draft Report Issued**	**Comments**
VAT	As agreed with the Section 151 Officer, this piece of work will be delayed due to additional work required to sign-off the Statement of Accounts.				
Green Waste					Due to be completed by Lancashire County Council in Q4
Payroll	Final Report Issued August 2019	Limited			Follow-up review to be completed December 2019
Pre-Employment Checks	Final Report Issued August 2019	Substantial			No post audit review necessary
Local Authority Trading Companies work					
• Trade Waste • Salt Ayre • Housing Company	At the time of reporting, no audit work had been completed in respect of LATC in the three areas. The audit team will monitor the progress being made and decide how audit will be best placed to add value to the process going forward.				
Project Assurance Work					
Procure to Pay (P2P)	The Principal Auditor has been attending regular project meetings and is involved in monitoring the performance data for this project. The group has recently focused on ensuring the segregation of duties and authorisation levels are correct. On-going monitoring will continue to ensure the project continues to progress and key controls are addressed as and when identified.				
Payroll Budget / E Budgeting	The Principal Auditor has attended a number of workshops and meetings and progress continues to be made.				
Follow-up work completed in 2019/20					
White Lund Nursery Income Management	Final Report Issued August 2019	Substantial			No post audit review necessary
Learning and Development	Final Report Issued August 2019	Substantial			No post audit review necessary
Performance Management	Whilst there has been good progress with implementation of the agreed action plan, a number of key actions are still in the process of being implemented, however this will continue to be the case whilst Cabinet and the council's priorities continue to develop and success measures are updated accordingly to align with these prioritise.				
Procurement and Contract Management	It has been agreed that the follow-up review for this piece of work and the Creditor follow-up review will be completed following the implementation of the Procure to Pay (P2P) project which is currently on-going. The implementation of P2P will heavily impact the controls around purchasing and payments.				
Dog Seizure and Kennelling Service	Following a follow up meeting with the Senior Environmental Health Officer (Community Protection) and the Community Health and Protection Officer (CHPO) it was identified that very little progress has been made in implementing the agreed actions. The Senior Auditor has agreed with the CHPO that the implementation target dates will be extended to January 2020 on the understanding that, all actions will have been addressed sufficiently enough to raise the assurance level to substantial. Failing this,				

	Report Status				
Category of Audit	**Final Report Issued**	**Assurance Level**	**Fieldwork**	**Draft Report Issued**	**Comments**
	the CHPO will attend the February Audit Committee meeting. The Director of Communities and the Environment has been informed of this.				
Council Housing – Asbestos Management	Final Report Issued May 2019	Moderate			Post audit review due November 2019
Creditors	Final Report Issued May 2019	Limited			See note above on Procurement and Contract Management
Asset Management	This piece of work was first complete in December 2017 and received a limited assurance opinion. A follow-up review was completed in December 2018 by the previous Principal Auditor and still received a limited assurance opinion. Following this, a further updated position was sought in August 2019 and it was found that no further progress had been made in implementing the agreed actions. The Senior Auditor has agreed with the Senior Property Officer that the implementation target dates will be extended to January 2020 on the understanding that, all actions will have been addressed sufficiently enough to raise the assurance level to substantial. Failing this, he will attend the February Audit Committee meeting. The Director of Economic Growth and Regeneration has been informed of this.				
Financial systems work					
Overtime and Holiday Pay					Due to be completed by Lancashire County Council
Assurance work requested					
Fixed Asset Register			✓		Due to be completed by Lancashire County Council
Property Investment Strategy			✓		
Debt Recovery					Due to be completed by Lancashire County Council
Planning Education Contributions			✓		
Service specific work					
Vehicle Maintenance Unit (Fleet Management)	August 2019	Limited			Post audit review due December 2019
Dog Warden Enforcement					Will be completed in Q4
Revenue shared service financial systems					
Council Tax – Preston (Occupation Validations)	October 2019	Substantial			No post audit review necessary
Council Tax – Lancaster (Occupation Validations)	October 2019	Substantial			No post audit review necessary

	Report Status				
Category of Audit	**Final Report Issued**	**Assurance Level**	**Fieldwork**	**Draft Report Issued**	**Comments**
Housing Benefits – E Claims					Will be completed in Q4
Other areas of work					
GDPR Compliance					This piece of work will be completed by an external body
National Fraud Initiative	Data files were uploaded in December 2018 and matches received are still in the progress of being reviewed. This is being continually monitored by Principal Auditor. The exercise in respect of the annual Single Person Discount will commence in December 2019 with the results being released in February 2019. The Corporate Fraud Manager will report on the findings of both exercises in his annual report to the Audit Committee.				
Supporting Corporate Enquiry Team (CET)	No specific work has been completed since 1 April 2019, however the team continue to support the CET as and when needed.				
Ethical Governance Survey	An ethical governance survey has been completed by the Internal Audit Team to test staff knowledge and understanding of the Council's key counter fraud policies. An action plan of the findings and any subsequent actions required to address any gaps in knowledge and understanding has now been published on Elsie.				
Counter Fraud and Corruption Policies	The Council has a number of counter fraud polices in place across the organisation, namely; Raising Concerns at Work (Whistleblowing) Policy, Gifts, Hospitality and Registering Interests Policy, Anti-Money Laundering, Corporate Prosecution Policy and the Anti-Fraud, Bribery and Corruption Policy. Whilst some of these polices are managed and reviewed by the Internal Audit Team and the Corporate Enquiry Team, and are therefore subjected to regular review and approval by the Audit Committee, some sit with other services, e.g. Human Resources and Democratic Services and therefore may not be subject to regular review and approval. Given the Audit Committee have delegated responsibility for ensuring adequate counter fraud arrangements are in place throughout the organisation, and Internal Audit is an independent, objective body, it was agreed as part of the Annual Governance Statement action plan that all the council's counter fraud policies, should sit with the Corporate Enquiry Team to ensure they are regularly updated, approved and rolled out to all staff. The above policies have all now been reviewed and will be presented to Audit Committee in February 2020 for approval.				
Embedding Risk Management	Work is currently underway to strengthen the council's risk management processes across the organisation. The draft Risk Management Policy and Strategy was submitted to the Audit Committee on the 27 November 2019. Following approval, work over the next 12 months will include the roll out of the Policy and Strategy, risk management training, shortly followed by the implementation of both strategic and operational risks registers. To ensure progress continues, risk management has been identified as a corporate project and regular updates are submitted to the Programme Board on a monthly basis.				

2.0 Investigations / other activity

2.1 To date, there have been no formal investigations carried out during 2019/20 that have required Internal Audit assistance.

3.0 Annual Governance Statement (AGS) 2018/19 Action Plan update – November 2019

A - Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law			
Behaving with integrity			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	**Update as at November 2019**
A1. Numerous procedural gaps within the Code of Conduct have been identified over time.	A1. The ongoing constitutional review (which started on the 31/3/19) will include review of Codes of Conduct, links to values and behaviours, scheme of delegation etc. In addition, an annual constitutional review is required to ensure it remains up to date	A1. Acting Head of Legal/ Monitoring Officer – 31 March 2020	Acting Head of Legal/ Monitoring Officer & Deputy Monitoring Officer in process of continuous review.
A2. Not embedded - The induction process does not currently cover Our Values, this needs to be embedded.	A2. Need to embed Our Values in the HR life cycle (appointment, inductions, target setting and appraisal processes) this is to include members. Union engagement will be sought on how this is to be achieved. The induction programme for new staff is to include ethics and values and this is to be carried out once the new HR Manager is in post.	A2. Head of HR – 31 March 2020	Not yet implemented – Estimated date for completion 31 March 2020.

A3. Parish Councillors do not receive any training on the Code of Conduct.	A3. The Monitoring Officer is to ensure Parish Councils are offered appropriate training.	A3. Acting Head of Legal/ Monitoring Officer – 31 October 2019	Change of personnel has meant this has not yet been offered. Monitoring Officer & Deputy Monitoring Officer to review the position and offer training when possible.
A4. A register of interests policy is in place for both staff and members.	A4. A register of interests is in place but is not frequently updated. In addition NIL responses are not always retuned as requested.	A4. Democratic Services Manger – 31 December 2019	Members have all updated their interests following the May elections. Following the identification of politically restricted staff, the Democratic Services Manager will now contact each officer asking them to submit a new declaration form.
A6. Need clarity on what should / should not be listed in the Gifts and Hospitality Register.	A6. Review / revise current registers and provide clarity through training & revisit thresholds.	A6. Democratic Services Manager – 31 March 2020	Thresholds for Members was increased from £25 to £50. The Democratic Services Manager will put together a short training clip for the intranet to be uploaded in December.

A8. The Anti-Fraud and Corruption polices & the fraud response plan are out of date. The Corporate Prosecution Policy is currently being updated by Legal Services.	A8. Establish responsibility for fraud polices and update. Approval by Audit Committee.	A8. Internal Audit and Assurance Manager / Fraud Manager – November 2019	Completed. All the Council's Counter Fraud Policies now sit under the Corporate Fraud Team and hopefully will be approved by the Audit Committee at their meeting on the 19 February 2020. All counter fraud policies will be reviewed annually.
A9. The Raising Concerns Policy is out of date – last reviewed Jan 2015.	A9. The raising concerns policy needs to sit independently with the Internal Audit and Assurance Team, alongside other counter fraud polices and be reviewed annually and approved by the Audit Committee.	A9. Internal Audit and Assurance Manager / Fraud Manager – 30 November 2019	Completed – See above
Demonstrating strong commitment to ethical values			
A12. Ethical Governance Survey and report completed but needs to be reviewed by Audit & Assurance Manager.	A12. The report on the results of the Ethical Governance Survey will be published following review by the Executive Management Team.	A12. Internal Audit and Assurance Manager – 31 August 2019	Completed.
A13. Guidance procedures for external funding and accountable bodies are documented within the Financial Regulations however these need to be reviewed.	A13. Guidance procedures for external funding and accountable bodies are documented within the Financial Regulations need to be reviewed to ensure they are fit for purpose and allow the organisation to function accordingly.	A13. Financial Services Manager – 31 December 2019	Not yet implemented – Estimated date for completion 31 December 2019.
A15. The Procurement policy is out of date and does not take account of the new values and ethical behaviour.	A15. The Procurement Policy is to be updated and take account of the new values and ethical behaviours.	A15. Procurement Manager – 31 December 2019	Not yet implemented – Estimated date for completion 31 December 2019.
A17. Staff appointments are made taking account of Our Values and not	A17. This new way of working needs to be developed, agreed, documented within	A17. Head of HR – 4 October 2019	A Values Based Competency agreement

just skills based however, these are not documented within any policy.	the appropriate policies and implemented across the Council, with training provided for recruiting managers		has been agreed in principle by the Executive Team. It is to be approved by Personnel Committee on the 15 October, it can then can be rolled out.
A18. Although the Council has an agreed Overview and Scrutiny work programme, there are issues in relation to the current lack of capacity to deliver the programme.	A18. Following the Election and the appointment of a Chair, the Principal Democratic Services Officer will work with the Chair on delivery of the scrutiny work programme.	A18. Democratic Services Manager – 31 October 2019	Completed.
A19. New guidance for HIA was published in April 2019, however need to ensure compliant.	A19. Need to ensure compliant with the new HIA guidance published in April 2019.	A19. Internal Audit and Assurance Manager / Financial Services Manager – 30 September 2019	Completed – The HIA is compliant with the new guidance.

A25. S151 advises that he does not always receive reports early enough to provide a thorough response.	A25. Introduction of electronic clearance of reports on Modgov will improve this.	A25. Democratic Services Manager – 31 March 2020	This is currently being delayed due to ICT issues, namely; No laptops for Committee staff, members can not access exempt papers due to the app not being installed and Mod Gov report clearance is not opening the blank template. It is expected that these issues will be resolved in the next few months.
A26. No register/record is held documenting advice and guidance provided by Legal.	A26. Legal are implementing a case management system in 2019/20, which will ensure all Legal advice given is recorded.	A26. Acting Head of Legal/ Monitoring Officer – 30 September 2019	Completed. Case Management System (IKEN) implemented. Ongoing training to staff on system.

B – Ensuring openness and comprehensive stakeholder engagement			
Openness			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
B8. Need to improve standard report pro-formas to facilitate decision making.	B8. Training on report writing will be rolled out when e-clearance comes in to place on Modgov.	B8. Democratic Services/HR Manager – 31 January 2020	Not yet implemented – Estimated date for completion 31 January 2020.
Engaging comprehensively with institutional stakeholders			
B16. No Partnership framework in place setting out any principles to assist officers when entering into partnership working	B16. Financial Regulations needs to include guidance on partnership working principles but these are not to be prescriptive.	B16. Financial Services Manager – 31 December 2019	Not yet implemented – Estimated date for completion 31 December 2019.

C - Defining outcomes in terms of sustainable economic, social and environmental benefits			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
C1. A new business planning template was trialled during 2017/18 which aligned with the new Council Plan. Services are currently identifying 'big ticket items' and then monitoring through performance reporting and individual appraisals.	C1. Internal Audit to liaise with Directors / Service Managers in 6-12 months to ensure compliance and consistency.	C1. Internal Audit and Assurance – 1 April 2020	Not yet implemented – Estimated date for completion 1 April 2020.
C2. Although KPI's are reported regularly the whole performance management reporting cycle needs to be reviewed.	C2. The Performance Management reporting framework is in the process of being refreshed to ensure that financial and key performance information is incorporated into the Road to Ambitions document.	C2 Financial Services Manager / Executive Support Manager / Programme Manager – 31 December 2019	Quarterly monitoring of performance, projects and resources has been integrated into a combined 'Delivering Our Ambitions' report to provide a joined up view of progress and a clearer reporting cycle. The next stages of the cycle's development are: - Further integration of performance, project and resource data so success measures are focused on outcomes rather than activities - Moving all information to an

			open, interactive platform to enable ready access and informed dialogue - Collating benefits, measures and timescales for all corporate projects alongside regular progress updates The regular update reports for corporate projects includes sections for the project lead to feedback on progress against the project plan, costs and benefits. All project leads have been asked to submit the benefits, measures and timeframes to achieve the benefits so that as projects complete and close they can be used to measure their success.

D - Determining the interventions necessary to optimise the achievement of the intended outcomes			
Determining interventions			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
D1. Not completed any report author training and guidance to assist report authors.	D1. Templates for reports require amending. Once completed these will be rolled out with training and guidance for report authors.	D1. Democratic Services Manager – 31 January 2020	Options have been sourced and demonstrated to the Executive Team. They have yet to make a decision as they need to consult with Cabinet.
D6. Monitoring of the Council's Plan and Ambitions document needs improving.	D6. Monitoring of the Council Plan should be conducted through the principles established in a refreshed Performance Management Framework.	D6. Financial Services Manager / Executive Support Manager / Programme Manager – 31 December 2019	The new 'Delivering Our Ambitions' report (see C2) provides a link between strategic ambitions and corporate performance, projects and resources, with further development in each area as follows: - Review of performance measures to accompany Outcome-Based Budgeting and development of Cabinet's updated priorities - Programme Board meets monthly to discuss progress of corporate projects

			- Outcome-Based Budgeting activity will inform future financial monitoring against member-agreed priorities As per C2, this activity will be supported by moving to an interactive platform, so monitoring can take place from day to day rather than at quarterly intervals. The Programme Board had its first meeting in July 2019 and continues to meet monthly to discuss progress made on corporate projects which form a significant part of the Council's Ambitions document. The highlight report discussed by the board and the individual update reports relating to each corporate project will shortly be available via the new intranet for all staff and members to view. The information is updated on a monthly basis.

E - Developing the entity's capacity, including the capability if its leadership and the individuals within it			
Developing the entity's capacity			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
E1. There is no workforce plan and/or organisational development plan in place.	E1. A workforce plan needs to be developed, taking into account current and planned measures.	E1. HR Manager – 31 January 2020	Organisational Development is now on a corporate project plan and strategic workforce planning is being designed and will be rolled out by the end of the year.
E8. The pay and grading structure for employees (referred to as the Job Evaluation system) is currently under review.	E8. We are currently finalising the agreement on the way forward. It is expected that a full JE process will be carried out during 2019/20	E8. HR Manager – Qtr 1 2020	The first phase of JE has been completed. The pay and grading structure model has been approved in principle with the Executive Team. Following review by the JCC and Personnel Committee it will then go to Full Council for approval.
Developing the capacity of the entity's leadership and other individuals			
E10. Financial Regulations and Financial Procedure Rules are reviewed should be annually reviewed by the Audit Committee but aren't currently.	E10. An annual review of the Financial Regulations will programmed into the Audit Committee work programme following the completion of the Constitutional review.	E10. Internal Audit and Assurance Manager / Financial Services Manager – 30 September 2020.	Not yet implemented – Estimated date for completion 31 September 2020.
E16. No competency framework in place. Our Values have not been embedded into the recruitment and selection and appraisal processes.	E16. Need to implement a framework that ensures the organisation applies Our Values consistently. See Principle A2	E16. HR Manager – 31 March 2020	See comments at A2

F - Managing risks and performance through robust internal control and strong public financial management			
Managing risks			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
F1. Risk Management is not yet thoroughly embedded into the culture of the Authority. The Risk Management Policy was approved by the Audit Committee several years ago, however has never been reviewed since	F1. The policy will be refreshed and approved by the Audit Committee. Following this, training will be provided for both officers and elected members ensuring that risk management is embedded across the Authority.	F1. Corporate Director of Resources / Internal Audit and Assurance Manager – Ongoing	Ongoing. A draft Risk Management and Strategy was submitted to the Audit Committee on the 27 November 2019. Following approval an external trainer will be identified to assist in the training of staff and Members.
F2. The Council has recently drafted a strategic risk register which has been viewed by the Audit Committee, there are currently no operational / service risk registers.	F2. Both Strategic and operational risk workshops will take place to ensure all key risks are documented and mitigating controls are put in place to protect the council and its services.	F2. Internal Audit and Assurance Manager – 1 April 2020	Not yet implemented – Estimated date for completion 31 April 2020.
Robust internal control			
F12. It was identified following the PSIAS review that the effectiveness of the Audit Committee has never been reviewed.	F12. A review of effectiveness will be carried out following the election of the new committee in May 2019.	F12. Internal Audit and Assurance Manager – 30 November 2020	A review of effectiveness will be carried out in November 2020, allowing the new Audit Committee Members to complete a complete cycle of the audit work programme.
F17. There is currently no Deputy Money Laundering Officer at the Council.	F17. Need to identify if a DMLO is required.	F17. Internal Audit and Assurance Manager – 31 December 2019	The Money Laundering Policy has been refreshed and is due to go to Audit Committee in November. The new DMLO is the Head of

			Financial Services and the Deputy DMLO is the Principal Accountant.
F18. It is acknowledge that although the Council has adopted a 'Local Code of Corporate Governance' this has not been refreshed to reflect the requirements of the 2016 Delivering Good Governance' framework.	F18. The Council needs to refresh the Code ensuring it reflects the 2016 'Delivering Good Governance' framework.	F18. Internal Audit and Assurance Manager – 31 December 2019	Not yet implemented – Estimated date for completion 31 December 2019.
Managing data			
F24. The Council's Records Management Policy needs to be reviewed/updated as it is out of date.	F24. Records management Policy is to be reviewed.	F24. Information Governance Manager – 1 February 2020	Not yet implemented – Estimated date for completion 1 February 2020.

G - Implementing good practices in transparency, reporting and audit, to deliver effective accountability			
Implementing good practice in transparency			
Weakness Identified	**Action Needed**	**Officer Responsible / Timescale**	
G1. The Council has not updated the required data in accordance with the Local Government Transparency Code 2015, since January 2019.	G1.In light of the update to the S45 Code of the FOI code of Practice, the Information Governance Manager has scheduled a review of the Council's FOI publication scheme within this financial year.	G1. Information Governance Manager – 1 April 2020	Not yet implemented – Estimated date for completion 1 April 2020.
G3. Individual services are responsible for keeping the website up to date, however the review dates are not always used, therefore information can be out of date.	G3. Regular reminders need to be issued to officers with responsibility for updating content on the Internet to ensure it is up to date and accurate.	G3. Communications Officer (Web and E-Marketing) – 1 August 2019	Completed and ongoing. Regular reminders are issued to content authors to check links and information on the website and there have been no reported issues in the last three months.
Assurance and effective accountability			
G16. The council's RIPA Policy does not include the procedure for using social media to carry out surveillance.	G16. The Council's RIPA Policy needs updating to reflect the council's procedure for using social media to carry out surveillance.	G16. Information Governance Officer – 1 April 2020	The Council's RIPA Policy has been updating to reflect the council's procedure for using social media to carry out surveillance. It was presented to the Audit Committee on the 27 November 2019
G17. The RIPA Policy and associated guidance is not easy to locate on the Intranet and RIPA training has not been provided for a number of years.	G17. The RIPA Policy and associated guidance will be made more readily available and training will be provided for all officers who carry out and/or authorise RIPA applications.	G17. Information Governance Officer - 1 January 2020	Not yet implemented – Estimated date for completion 1 January 2020.

4.0 Details of Consultation

4.1 Management Team and Service Managers continue to be consulted in delivering both the audit plan and the Annual Governance Statement action plan.

5.0 Options and Options Analysis (including risk assessment)

5.1 There are no other options available.

6.0 Conclusion

6.1 The programme of audits for the rest of the year continues to be implemented in consultation with Service Managers.

6.3 The Annual Governance Statement action plan will continue to be monitored by Internal Audit and Management Team.

CONCLUSION OF IMPACT ASSESSMENT (including Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing) Not applicable
FINANCIAL IMPLICATIONS None directly arising from this report
SECTION 151 OFFICER'S COMMENTS The Section 151 Officer has been consulted and has no further comments
LEGAL IMPLICATIONS None directly arising from this report
MONITORING OFFICER'S COMMENTS The Monitoring Officer has been consulted and has no further comments

BACKGROUND PAPERS Internal Audit Plan 2019/20 Annual Governance Statement 2018/19	**Contact Officer:** Joanne Billington **Telephone:** 01524 582028 **E-mail:** jbillington@lancaster.gov.uk **Ref:**

AUDIT COMMITTEE

Review of the Council's Risk Management Policy
27 November 2019

Report of the Internal Audit and Assurance Manager

PURPOSE OF REPORT
To review and approve the council's refreshed Risk Management Policy.
This report is public

RECOMMENDATIONS

1. That the Audit Committee is asked to review and approve the refreshed Risk Management Policy at Appendix A.

1.0 Introduction

1.1 The Risk Management Policy is a key document, which identifies the council's approach to risk management, and demonstrates how it is embedded across the council.

1.2 In accordance with their terms of reference the Audit Committee is charged in providing those with governance, independent assurance of the adequacy of the risk management framework. This will involve monitoring the effective development and operation of risk management across the council and monitoring progress in addressing risk-related issues reported to the committee.

1.3 The council's Risk Management Policy was first adopted on 16 December 2003 and was subsequently reviewed and updated with fairly minor amendments on three occasions; namely, July 2005, June 2007 and May 2008. Following an Internal Audit review of Risk Management in March 2009 it became apparent that a much more substantial review was necessary. Subsequently, the Risk Management Policy and other associated guidance was replaced with, a consolidated 'Code of Practice for Managing Risk and Opportunity – A Sense of Proportion' which was approved by the Audit Committee on the 22 April 2009.

1.4 Since 2009, whilst there are a number of good examples across the organisation where it can be demonstrated that robust risk management has been applied to its decision making process, it is still felt that more work is required to ensure risk management is embedded throughout the organisation. Work over the next 12 months will include the roll out of the attached policy, risk management training, shortly followed by the implementation of both strategic and operational risks registers. To ensure progress continues, risk management has been identified as a corporate project and regular updates are submitted to the Programme Board on a monthly basis.

2.0 Details of consultation

2.1 No specific consultation has been undertaken in compiling this report.

3.0 Options and options analysis (including risk assessment)

3.1 No alternative options were identified.

4.0 Conclusion

4.1 The adoption of this policy will help the council to demonstrate its commitment to a policy of managing risk wherever it may arise.

4.2 The council's refreshed Risk Management Policy is attached at Appendix A.

CONCLUSION OF IMPACT ASSESSMENT (including Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing) This report has no direct impact on these areas.
FINANCIAL IMPLICATIONS None arising directly from this report.
SECTION 151 OFFICER'S COMMENTS The Section 151 Officer has been consulted and has no further comments.
LEGAL IMPLICATIONS None arising directly from this report.
MONITORING OFFICER'S COMMENTS The Monitoring Officer has been consulted and has no further comments.

BACKGROUND PAPERS None	**Contact Officer:** Joanne Billington **Telephone:** 01524 582028 **E-mail:** jbillington@lancaster.gov.uk **Ref:**

Appendix A

LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

Risk Management Policy

November 2019

Version 1.01

Contents

1.0 Introduction
2.0 Scope
3.0 Risk Management Objectives
4.0 Benefits
5.0 Definitions
6.0 Standards
7.0 Approach
8.0 Risk Registers
9.0 Roles and Responsibilities
10.0 Embedding Risk Management
11.0 Culture
12.0 Training and Awareness
13.0 Summary

Appendix 1 - Check List for Risk Identification
Appendix 2 - Measures of Likelihood and Impact
Appendix 3 - Risk Response Categories

Version control

	Description	**Date**
1.01	Draft submitted to Executive Team for comments	13 November 2019

1.0 Introduction

1.1 Risk is unavoidable and is part of all our lives. As an organisation, we need to take risks to grow and develop. Risk management involves understanding, analysing and addressing risks to make sure the organisation achieves its objectives. Successful risk management can make a council more flexible and responsive to new pressures and external demands. It allows an organisation to deliver services better and to meet the needs and expectations of its community in what is a fast changing and dynamic environment. The benefits of successful risk management include, improved service delivery, financial performance and corporate governance.

1.2 This policy explains Lancaster City Council's approach to risk management and the framework that will operate to establish and drive an effective system not only to minimise risk but also to enable continuous improvement at every level of the organisation.

2.0 Scope

2.1 This policy applies to all staff, the council's elected Members and all working groups and partnerships. The responsibilities of these groups and the individuals within them, for the implementation and the effective management of risk is detailed below.

2.2 This policy and guidance will be reviewed periodically to take account of changing legislation, government initiatives, best practice and experience gained within the council.

3.0 Risk Management Objectives

3.1 The council has identified a number of key risk management objectives that need to be met to ensure a robust risk management framework is embedded across the council; namely:

- Adopt a strategic approach to risk management to make better informed decisions which is vital to successful transformational change;
- Set the 'tone from the top' on the level of risk we are prepared to accept on our different service delivery activities and priorities;
- Acknowledge that even with good risk management and our best endeavours, things can go wrong. Where this happens we use the lessons learnt to try to prevent it from happening again;
- Develop leadership capacity and skills in identifying, understanding and managing the risks facing the council;
- Integrate risk management into how we run council business/services. Robust risk management processes help us to achieve our core purpose, priorities and outcomes;
- Support a culture of well-measured risk taking throughout the council's business. This includes setting risk ownership and accountabilities and

responding to risk in a balanced way, considering the level of risk, reward, impact and cost of control measures;

- Ensure that the council continues to meet all statutory and best practice requirements in relation to risk management; and

- Ensure risk management continues to be a key and effective element of our Corporate Governance arrangements.

4.0 Benefits

4.1 In addition to supporting strategic and operational business planning, if risk management is thoroughly embedded and practices are consistently applied it can bring a number of other key benefits to the organisation, namely;

- Improved service delivery and financial performance, supporting the effective use of the council's resources;
- Improved decision making and budgeting;
- Continuous service improvement; and
- Enhanced communication between staff, Elected Members and partners.

5.0 Definitions

5.1 Risk can be defined as;

"An uncertain event that, should it occur, will have an effect on the council's objectives and/or reputation. It is the combination of the probability of an event (likelihood) and its effect (impact)".

Risk management can be defined as;

"The systematic application of principles, approach and processes to the identification, assessment and monitoring of risks."

5.2 By managing our risk process effectively we will be in a better position to safeguard against potential threats and exploit potential opportunities to improve services and provide better value for money.

5.3 Risk management is applied at all levels of service delivery across the council. The council separates risk into two categories;

Corporate Strategic Risks – Risks that could have an effect on the successful achievement of our long term core purpose, priorities and outcomes. These are risks that could potentially have a council-wide impact and/or risks that cannot be managed solely at a service level because higher level support/intervention is needed.

Operational / Service Risks – Risks that could have an effect on the successful achievement of the service or business outcomes / objectives. Potentially these risks could have a significant financial, reputational and/or service delivery impact on the business unit as a whole.

6.0 Risk Management Standards

6.1 A number of standards have been developed worldwide to help organisations implement risk management systematically and effectively. These standards seek to establish a common view on frameworks, processes and practice, and are generally set by recognised international standards bodies or by industry groups. Risk management is a fast-moving discipline and standards are regularly supplemented and updated.

6.2 Despite the publication of the global risk management standard in 2009; ISO 31000, the Institute of Risk Management (IRM) has decided to retain its support for the original 'Risk Management Standard' that was published in 2002 because it is a simple guide that outlines a practical and systematic approach to the management of risk. The standard is not prescriptive i.e. a box ticking exercise or a certifiable process. Instead, the standard represents best practice against which organisations can measure themselves. The council has reviewed this policy against this standard.

7.0 Risk Management Approach

7.1 The purpose of the risk management approach outlined in this Policy is to:

- Provide standard definitions and language to underpin the risk management process;
- Ensure risks are identified and assessed consistently throughout the organisation through the clarification of key concepts;
- Clarify roles and responsibilities for managing risk; and
- Implement an approach that meets current legislative requirements and follows best practice and relevant standards.

7.2 Before we can identify our risks we need to establish the context by looking at what we are trying to achieve and what our proposed outcomes are. Depending on the area under review, the relevant objectives and outcomes will usually be detailed in existing documents, e.g. council plan, individual services plans, project briefs, partnership agreements etc.

To ensure consistency, the following four steps should be followed when identifying, evaluating, treating / mitigating and reviewing risks;

Step 1 – Identifying risk

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all risks flowing from these activities have been defined. The majority of risks will be identified as part of the routine service planning stages where barriers to specific business objectives can easily be recognised. All staff have a duty to report emerging risks to their heads of service / manager as and when they are identified. Risks can arise and be identified when the following events occur:

- the change of internal or external processes;

- staff/councillors leave and/or restructuring takes place;
- through procurement of a new supplier or asset;
- partners change or are re-structured;
- legislation is revised or introduced;
- the social and or economic climate alters; or
- an incident occurs.

To help in the risk identification process a number of common risk assessment techniques/methods can be used, for example, questionnaires, checklists, workshops, brainstorming sessions, audits and inspection reports or flowcharts.

There are a number of different types of risks that an organisation may face including financial loss, failure of service delivery, physical risks to people, and damage to the organisation's reputation. To act as a prompt and to ensure completeness, a checklist of risk categories has been developed around the acronym '**PERFORMANCE'**. Examples of risks from each category are detailed in the Risk Identification Checklist at Appendix 1.

When describing risks, it helps to display the identified risk in a structured format to ensure a comprehensive risk identification, description and assessment process takes place. The council has developed a corporate format which must be used to identify, evaluate and mitigate risk. Templates can be located on the intranet.

Once identified, all risks are recorded in a 'Risk Register'. A risk owner must be allocated and recorded against each risk on the risk register. Such accountability helps to ensure 'ownership' of the risk is documented and recognised. A risk owner is defined as a person with the accountability and authority to effectively manage the risk. At this stage there may well be a long list of possible risks. The next step will help to prioritise these in order of importance.

Step 2: Analysing and Evaluating risk

In order to analyse and evaluate risks, a thorough risk assessment needs to be undertaken. That is, a detailed analysis of the potential threats faced by the council which may prevent achievement of its objectives. Through consideration of the sources of the risk, possible consequences, and the likelihood of those consequences occurring, it helps make decisions about the significance of risks and whether they should be accepted or treated.

The council will firstly consider the gross (inherent) risk to ensure that informed decisions can be made about the consequences of stopping risk actions that are currently in place; and resources are not wasted over-controlling risks that are not likely to happen and would have little impact.

Following identification of the risk, a score for the likelihood and impact will be given to the risk as it currently stands, taking into consideration any controls already in place and/or any existing actions that are not operating effectively. The total risk score will be the deciding factor if further action is required.

A "traffic light" approach is used to show high (red), medium (amber) and low (green) risks. To ensure resources are focused on the most significant risks, the council's approach to risk management is to focus on the risks that have

scored as ‘red’ on the matrix. This may also be referred to the council’s risk appetite.

Any risks that are NOT scored as a ‘red’ risk, therefore falls below the risk appetite, will be accepted and kept under review for any significant changes that may increase the risk score. Anything identified as a ‘red’ risk will take priority and the necessary actions will be taken to mitigate the risk.

To ensure that a consistent scoring mechanism is in place across the council, risks are assessed using the agreed criteria for likelihood and impact detailed in Appendix 2. When assessing the risk, the highest measure identified in each table is the score taken to plot the risk level on the risk matrix (Diagram 1). The likelihood and impact crosses, determines the risk level. For example, Possible Likelihood (2) and Very High Impact (4) would result in a risk level of 8.

Step 3: Treatment and Action Planning

Actions, which will help to minimise the likelihood and / or impact of the risk occurring, are identified for each ‘red’ risk. A risk owner should be identified for each action. A second risk score should then be given to identify the ‘net (residual) risk that still remains after taking into account the mitigating actions/controls.

Net risks are prioritised by applying the same criteria and matrix used for assessing the gross risk level (Step 2). It is the risk owner’s responsibility to ensure that the agreed net risk level for each risk is an accurate reflection of the likelihood and impact measures detailed in Appendix 2.

Not all risks can be managed all of the time, so having assessed and prioritised the identified risks, cost effective action needs to be taken to manage those that pose the most significant threat.

Risk may be managed in one, or a combination of, of the following ways:

- Avoid - A decision is made not to take a risk;
- Accept - A decision is taken to accept the risk;
- Transfer - All or part of the risk is transferred through insurance or to a third party;
- Reduce - Further additional actions are implemented to reduce the risk; or
- Exploit - Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.

These are described in more detail in Appendix 3. The managed approach to risk should always be documented in the risk register, for example, after the first assessment of the risk, a decision may be made to ‘transfer’ the risk, therefore no further mitigating controls are required. This must be clearly stated in the register to evidence the effectiveness of the evaluation and scoring process. In another example, a decision may be made following the second assessment, that despite additional controls the residual risk is still too great and that a decision is made to avoid the risk entirely by stopping the activity. Again this must be clearly documented.

Step 4 – Monitoring and Reporting

Risk management should be thought of as an ongoing process and as such risks need to be reviewed regularly to ensure that prompt and appropriate action is taken to reduce their likelihood and/or impact.

Regular reporting enables senior managers and Members to be more fully aware of the extent of the risks and progression being made to manage them. The strategic risk register will be reviewed annually by the Executive Team via a risk workshop, and action plans will be updated quarterly. The operational risk registers will be reviewed annually by Heads of Service / Managers or the relevant Director and action plans will be updated on a quarterly basis.

Progress on high 'red' risks for both strategic and operational risk registers will be reported to the Audit Committee at each of their meetings (February, May, July and November).

8.0 Risk Registers

8.1 To ensure that the risk registers are comprehensive and accurately reflect the levels of risk within the council, all relevant and available sources of information will be used in their compilation and review, namely:-

- The council's Annual Governance Statement;
- Internal audit reports;
- External audit reports;
- Committee reports / portfolio holder / officer delegation reports;
- Risk Assessments;
- Incident / accident reports;
- Insurance claims and advice from the council's Insurers;
- Complaints; and
- Any relevant articles from risk management publications.

8.2 The Internal Audit and Assurance Team will maintain both strategic and operational risk registers. The registers will be held in spreadsheets which can be viewed on the council's intranet and will be used to monitor risk movements.

8.3 Amendments to risk scores (likelihood x impact) can only be actioned by the Internal Audit and Assurance Team after evidence of increased or improved control, or another viable explanation has been recorded e.g. the activity ceases altogether.

9.0 Roles and Responsibilities

9.1 To ensure risk management is effectively implemented, all staff and Members should have a level of understanding of the Council's risk management approach and regard risk management as part of their responsibilities:

All Employees

- ♦ Manage day to day risks and opportunities effectively and report risk management concerns to their line managers;
- ♦ Participate fully in risk workshops and action planning as appropriate; and
- ♦ Attend training and awareness sessions as appropriate.

All Members

- Support and promote an effective risk management culture; and
- Constructively review and scrutinise the risks involved in delivering the council's core purpose, priorities and outcomes.

Some individuals and groups have specific leadership roles or responsibilities and these are identified below:

Cabinet

- Risk manage the council in delivering its core purpose, priorities and outcome; and
- Consider and challenge the risks involved in making any 'key decisions'.

Audit Committee

- Provide independent assurance to the council on the overall adequacy of the risk management framework, including review of proposed amendments to the Risk Management Policy prior to its presentation to Cabinet;
- Review and challenge the content of risk registers;
- Where appropriate escalate operational risks for possible inclusion on the strategic risk register; and
- Approve and review recommendations and amendments to the Risk Management Policy.

The Executive Team

- Champion an effective council-wide risk management culture;
- Ensure Members receive relevant risk information; and
- Responsible for owning and managing corporate strategic risks.

Corporate Directors

- Risk manage their directorate in delivering the council's core purpose, priorities and outcomes;
- Constructively review and challenge the risks involved in decision making; and
- The Director of Corporate Services, supported by the Internal Audit and Assurance Manager champion's risk management. It is their responsibility to promote the adequate and proper consideration of risk management to senior managers and more widely within the council.

Heads of Service / Managers

- Responsible for the effective leadership and management of risk in their service areas to meet service objectives / outcomes in line with the council's risk management framework;
- With the appropriate risk owner, maintain the relevant risk registers ensuring all key risks are identified, managed and reviewed in line with the corporate risk management approach;
- Promptly escalate risks appropriately;
- Encourage staff to be open and honest in identifying risks and opportunities;

- Ensure risk management process is an explicit part of transformation and all significant projects;
- Ensure that appropriate resources and importance are allocated to the process; and
- Provide assurance that the risks for which they are the risk owner are being effectively managed. This will be completed as part of the Annual Governance review process.

Risk Owners

- Take ownership of the action/s they are responsible for by either confirming the existence and effectiveness of existing actions or ensuring that any further actions are implemented.

Partners

- Where appropriate participate in the development of a joint partnership risk register;
- Actively manage risk within the partnership; and
- Report on risk management issues to partnership boards or equivalent.

Internal Audit

- Design and facilitate the implementation of a risk management framework ensuring it meets the needs of the organisation;
- Act as a centre of expertise, providing support and guidance as required;
- Collate risk information and prepare reports as necessary to both the Executive Team and the Audit Committee;
- Ensure the Internal Audit work plan is focused on the key risks facing the council;
- Provide assurance that risks are being effectively assessed and managed;
- During all relevant audits, challenge the content of risk registers; and
- Periodically arrange for the independent review of the council's risk management process and provide an independent objective opinion on its operation and effectiveness.

10.0 Embedding Risk Management

10.1 For risk management to be effective and a meaningful management tool, it needs to be an integral part of key management processes and day-to-day working. As such, risks and the monitoring of associated actions should be considered as part of a number of the council's significant business processes, including:

- Corporate Decision Making – significant risks, which are associated with policy or action to be taken when making key decisions, are included in appropriate committee reports.

- Business / budget planning – this annual process includes updating the relevant risk registers to reflect current aims / outcomes.

- Project Management – all significant projects should formally consider the risks to delivering the project outcomes before and throughout the project. This includes risks that could have an effect on service delivery, benefits realisation and engagement with key stakeholders (service users, third parties, partners etc.).

- Partnership Working – partnerships should establish procedures to record and monitor risks and opportunities that may impact the council and/or the partnership's aims and objectives.

- Procurement – all risks and actions associated with a purchase need to be identified and assessed, kept under review and amended as necessary during the procurement process.

- Contract Management – significant risks associated with all stages of contract management are identified and kept under review

- Insurance – the council's Insurance Officer manages insurable risks and self-insurance arrangements.

- Health and Safety – the council has specific policies and procedures to be followed in relation to health and safety risks.

11.0 Culture

11.1 The council will be open in its approach to managing risks and will seek to avoid a blame culture. Lessons from events that lead to loss or reputational damage will be shared as well as lessons from things that go well. Discussion on risk in any context will be conducted in an open and honest manner.

12.0 Training and Awareness

12.1 Having documented a robust approach and established clear roles and responsibilities and reporting lines, it is important to provide officers and Members with the knowledge and skills necessary to enable them to manage risk effectively. The Internal Audit Team will use a range of training methods to meet the needs of the organisation. Furthermore, risk management information and templates will be developed and will be available on the intranet to ensure the council can apply a consistent approach when managing risk.

13.0 Summary

13.1 The adoption of this policy and the ongoing efforts to embed sound risk management principles into the council's 'fabric' will improve the way in which services are delivered. A solid, well-documented and comprehensive approach to risk management and its adoption into the decision making process is good practice, essential to good management and strengthens the council's governance framework.

Appendix 1

Check List for Risk Identification
(PERFORMACE)

Political

- Change in Government policy
- Member support / approval
- Political personalities
- New political arrangements

Economic

- Demographics
- Economic downturn - prosperity of local businesses / local communities

Regulatory

- Legislation and internal policies/regulations including:
  - Health & Safety at Work Act, Data Protection, Freedom of Information, Human Rights, Equalities Act 2010 and Public Sector Equality Duty 2011, Employment Law, TUPE, Environmental legislation etc.
- Grant funding conditions
- Legal challenges, legal powers, judicial reviews or public interest reports

Financial

- Budgetary pressures
- Loss of/reduction in income/funding
- Cost of living/inflation, interest rates, increase in energy costs
- Financial management arrangements
- Investment decisions, Sustainable economic growth
- Affordability models and financial checks
- Inadequate insurance cover
- System / procedure weaknesses that could lead to fraud

Opportunities/ Outcomes

- Add value or improve customer experience/satisfaction
- Reduce waste and inefficiency
- Maximising independence for older people with disabilities
- Developing sustainable places and communities
- Protecting the community and making Lancaster a safer place to live

Reputation

- Negative publicity (local and national), increase in complaints

Management

- Loss of key staff, recruitment and retention issues
- Training issues
- Lack of/or inadequate management support
- Poor communication/consultation
- Capacity issues - availability, sickness absence
- Emergency preparedness / Business continuity

Assets

- Property - land, buildings and equipment,

- Information – security, retention, timeliness, accuracy, intellectual property rights
- ICT – integrity, security, availability, e-government
- Environmental - landscape, countryside, historic environment, open space

New Partnerships/ Projects/ Contracts

- New initiatives, new ways of working, new policies and procedures
- New relationships – accountability issues / unclear roles and responsibilities
- Monitoring arrangements
- Managing change

Customers/ Citizens

- Changing needs and expectations of customers - poor communication/consultation
- Poor quality / reduced service delivery - impact on vulnerable groups
- Crime and disorder, health inequalities, safeguarding issues

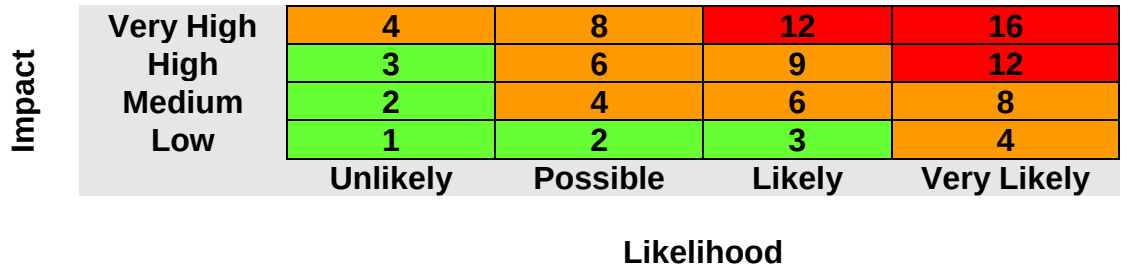
Environment

- Recycling, green issues, energy efficiency, land use and green belt issues, noise, contamination, pollution, increased waste or emissions,
- Impact of planning or transportation policies
- Climate change – hotter drier summers, milder wetter winters and more extreme events – heat waves, flooding, storms etc

Appendix 2

Measures of Likelihood and Impact

Diagram 1



Likelihood Measures

	Unlikely 1	Possible 2	Likely 3	Very Likely 4
Probability	**Less than 10%** chance of circumstances arising	**10% to 40%** chance of circumstances arising	**41% to 75%** chance of circumstances arising	**More than 75%** chance of circumstances arising
Timescale	Is **unlikely** to occur.	Possible in the **next 3 or more years**.	Likely to occur in the **next 1-2 years**.	Occurred in the **past year** or is very likely to occur in the **next year**.

Impact Measures

	Low 1	Medium 2	High 3	Very High 4
People / Duty of Care	Low level of foreseeable minor injuries	High level of foreseeable minor injuries Low level of foreseeable serious injuries	High level of foreseeable severe injuries	Foreseeable long-term injury, illness
Financial Impact	Up to £500k Less than 5% over project budget	Up to £2 million 5-10% over project budget	Up to £5 million 11-25% over project budget	Over £5 million More than 25% over project budget
Legal Impact	Minor civil litigation	Major civil litigation and/or local public enquiry	Major civil litigation and/or national public enquiry	Legal action certain Section 151 or government intervention or criminal charges
Service Impact	Short term service disruption	Noticeable service disruption affecting customers	Significant service failure but not directly affecting vulnerable groups	Serious service failure directly affecting vulnerable groups

Project Delivery	Minor delay to project	Significant delay to project	Project fails to deliver target impacting on the service performance	Project fails to deliver target impacting on council's performance
Intervention Required	Intervention by Service Manager, Project Manager or equivalent	Intervention by Head of Service or equivalent.	Intervention by the Executive or Board	Intervention by Boars or Council
Reputation Impact	Short term negative local media attention	Significant negative local media attention	Sustained negative local media attention and/or significant national media attention	Sustained negative national media attention

Appendix 3

Risk Response Categories

	Description
Avoid	A decision is made not to take a risk. Where the risks outweigh the possible benefits, avoid the risk by doing things differently e.g. revise strategy, revisit objectives or stop the activity.
Accept	A decision is taken to accept the risk. Management and/or the risk owner make an informed decision to accept that existing actions sufficiently reduce the likelihood and impact of a risk and there is no added value in doing more.
Transfer	Transfer all or part of the risk through insurance or to a third party e.g. contractor or partner, who is better able to manage the risk. Although responsibility can be transferred, in most cases accountability remains with the council, so this still needs to be monitored.
Reduce	Implement further additional action(s) to reduce the risk by; • minimising the likelihood of an event occurring (e.g. preventative action) and/or • reducing the potential impact should the risk occur (e.g. business continuity plans) Further actions are recorded in the risk register and regularly monitored.
Exploit	Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.