Wyre Borough Council
Date of Publication: 19 September 2022
Please ask for : Daphne Courtenage
daphne.courtenage@wyre.gov.uk
Tel: 01253 887476

Audit Committee Agenda

Audit Committee meeting on Tuesday, 27 September 2022 at 6.00 pm in the Committee Room 2 - Civic Centre

1. Apologies for absence

2. Declarations of interest

To receive any declarations of interest from any members of the Committee on any item on this agenda.

3. Confirmation of minutes (Pages 3 - 8)

To confirm as a correct record the minutes of the last meeting of the Audit Committee held on 14 June 2022.

4. Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA) (Pages 9 - 40)

Report of the Legal Services Manager, presented by the Legal Services Manager.

5. Annual Review of the Council's Risk Management Policy (Pages 41 - 62)

Report of the Corporate Director Resources (Section 151 Officer) presented by the Audit, Risk and Performance Lead.

6. Statement of Accounts (pre-audit) 2021/22 (Pages 63 - 66)

Report of the Corporate Director Resources (Section 151 Officer).

7. Exclusion of the public and press

The Chief Executive has determined, in accordance with Paragraph 11 of the Access to Information Rules in Part 4 of the Council's

Constitution, that the reports submitted under item 8 of this agenda are “Not for Publication” because they contain “exempt information”, as defined in Schedule 12A of the Local Government Act 1972.

If the Committee agrees that the public and press should be excluded for these items, it will need to pass the following resolution.

“That the public and press be excluded from the meeting whilst agenda item 8 is being considered, on the grounds that their presence would involve the likely disclosure of exempt information as defined in categories 3 and 5 of Part 1 of Schedule 12(a) of the Local Government Act, 1972, as amended by the Local Government (Access to Information) Variation Order 2006 and, that the public interest in maintaining the exemptions outweighs the public interest in disclosing the information”.

8. Draft Annual Governance Statement 2021-22 update (Pages 67 - 72)

Verbal update from the Corporate Director Resources (Section 151 Officer).

Attached to this item is the restricted report Cabinet considered at the meeting of 07 September 2022 to aid members in this discussion.

9. Periodic private discussion with External Audit

Following the conclusion of the formal meeting, members of the committee will be given the opportunity to have their private periodic discussion with the External Auditor, as provided for in the committee’s work programme.

Audit Committee Minutes

The minutes of the Audit Committee meeting of Wyre Borough Council held on Tuesday, 14 June 2022 at the Council Chamber - Civic Centre, Poulton-le-Fylde.

Audit Committee members present:
Councillors McKay, Ingham, A Turner, Fairbanks and Ibison

Apologies for absence:
Councillors E Ellison, George, Leech, Longton, Minto, Moon, Stirzaker, L Walmsley and Webster

Other councillors present:
None.

Officers present:
Daphne Courtenage Assistant Democratic Services Officer
Dawn Allen, Audit, Risk and Performance Lead
Joanne Billington, Head of Governance and Business Support
Clare James, Corporate Director Resources (S151 Officer)
Karen McLellan, Audit and Risk Manager

No members of the public or press attended the meeting.

---

1 Election of Chairman

Agreed that Councillor McKay be elected as Chair of the Audit Committee for the 2022/23 municipal year.

2 Election of Vice Chairman

Agreed that Councillor Ingham be elected as Vice-Chair of the Audit Committee for the 2022/23 municipal year.

3 Declarations of interest

None.

4 Confirmation of minutes

The minutes of the meeting of the Audit Committee held on the 1 March 2022 were **approved** as a correct record.

5 Review of Effectiveness of Internal Audit

The Corporate Director Resources (S.151 Officer) submitted a report that related to the requirement for the authority to undertake an annual review of the effectiveness of the system of internal audit, demonstrating that the council had an effective internal audit function.

The Audit and Risk Manager introduced the report.

She explained to the committee that the Accounts and Audit Regulations and the Public Sector Internal Audit Standards (PSIAS) required the council to review the effectiveness of internal audit once a year, to support the annual audit opinion and as a key piece of evidence in the Annual Governance Statement. She said that to assist with the review, CIPFA had published an application note along with a checklist to assist in measuring performance of the standards.
She told members that they had paid special attention to the review this year, as the results would be independently validated as part of their peer review, taking place in February 2023.

Following the review, she confirmed that internal audit were compliant with best practice and the PSIAS, with two minor areas highlighted which required more attention. These areas were: updating the Quality Assurance Improvement Plan, and the requirement to seek an independent review of the council's management processes owing to internal audit involvement in the management of this.

She recommended to the committee that they consider the results of the review of the effectiveness of Internal Audit. The committee considered the results of the review and did not have any comments on this report.

6 Annual Internal Audit Report 2022

The Corporate Director Resources submitted a report to support members in reviewing the Internal Audit Annual Report for 2021/22 and in reviewing progress in relation to risk management activity.

The Audit and Risk Manager introduced the report.

She explained to members that the internal audit report was produced to meet requirements set out by PSIAS and to assist in meeting the Accounts and Audit Regulations 2015. The report set out the progress made and work carried out in relation to internal audit and risk management for the year 2021/22. She told members that the outcomes of this work would allow her to make an annual, overall opinion in relation to internal control, risk management and the governance processes across the council.

She explained to the committee that owing to resourcing constraints, there was some work that had not been completed, with work on the two delayed areas being added to the audit plan for 2022/23. She also explained to members that Marine Hall had been added back onto the audit plan for 2022/23 as a result of its re-opening after its closure during the pandemic.

The Chair asked about the site inspections report, which had been given a 'Fair' rating by the Auditor and what processes were in place to complete this work. The Audit and Risk Manager explained that this work would be added to their GRACE Risk Management system, with actions to be followed up by officers and the internal audit team.

She also took the committee through the other audit work undertaken by the team during 2021/22, as detailed on pages 103-110 of the agenda pack. The Audit, Risk and Performance Lead explained the item on the National Fraud Initiative, updating members that they had trained the Corporate Apprentices and the Insurance and Business Continuity Officer to assist with the ongoing investigations from the 2020/21 council tax single person discount data matching exercise.

The Head of Governance and Business Support spoke to members on information governance and her judgement as Data Protection Officer on security and use of business assets. She stated that cyber security continued to be a concern, and a risk assessment was in progress. Despite the continued concerns around cyber security and larger pieces of work continuing on the council's information asset registers, she told members she was happy that both of these issues would be addressed.

The Audit and Risk Manager spoke to the committee on updates to the council's counter fraud policies; she reminded members that they had recently completed the Ethical Governance Surveys, which test users' knowledge and understanding of the council's counter fraud policies. The actions that arose through the survey were being addressed by Democratic Services, the majority of which were completed following the launch of the councilor portal. She also updated members on recent whistleblowing calls and informed the committee that the Audit Chair had been fully briefed on these.

Councillors asked questions on the discretionary policy for residents receiving the £150 council tax energy rebate payment. The Corporate Director Resources explained that there was a requirement for the council to have a discretionary policy for residents in bands E-H which would target residents in receipt of localised council tax support and other uses were being explored.

Following discussions on the Quality Assurance Improvement Plan (QAIP), the compliance of the PSIAS, and an update to the work of the Compliance team, the Audit and Risk Manager gave her annual opinion to members. She explained to members she was required to form an opinion on the adequacy and effectiveness of the council's internal control environment. She was pleased to present a positive report to the committee in light of the effect of the pandemic and other challenges, such as the new hybrid-working

arrangements. She said that improvements to their resources would have a positive effect on the PSIAS peer review in early 2023.

Her overall opinion was that 'reasonable assurances could be given on the overall adequacy and effectiveness of the council's governance risk management, and control processes'. The full opinion can be found at pages 31-32 of the report in the agenda pack.

In addition, the Audit and Risk Manager went through the risk management progress report for members. She told members that purchasing the risk management system (GRACE) enabled the team to automate the process and remove internal audit from the management and administration of risk, allowing them to give a more independent and objective opinion on the effectiveness of these processes.

Members considered the internal audit annual report, the risk management progress report, the strategic risk register and the ICT risk register.

7 Draft Annual Governance Statement 2021-22

The Corporate Director Resources (S151 Officer) submitted a report to assist members in reviewing and formally approving the draft annual governance statement (AGS) for 2021/22, for inclusion in the Annual Statement of Accounts.

The Head of Governance and Business Support introduced the report.

She explained to members that the council was required to publish an AGS along with a Statement of Accounts. She told members that this was a draft version, and there would be a gap of time between the approval of the draft and the official sign-off. The draft AGS was therefore subject to change or amendments.

The sign-off of the AGS formed part of the committee's terms of reference, and members were asked to review the statement in relation to the evidence that had been documented against each of the principles to demonstrate the council's governance framework. She informed members that the external auditors, Deloitte, would also scrutinise the draft AGS as part of their work.

She stated that no significant governance issues were raised that required documenting separately in the Annual Governance Statement for 2021/22 and that for the first time, members were receiving details on the minor issues that had been identified when pulling together the AGS.
She told members that following this meeting, the draft AGS would be issued to the Leader of the Council and the Chief Executive and asked to sign the AGS in agreement with it and that they were aware of the governance issues within the authority. Following this, it would be submitted into the Statement of Accounts.

The Head of Governance and Business Support also asked the committee to

give delegated authority to the Section 151 Officer to make minor amendments and any changes requested by the external auditors following their review during the time between the approval of the draft AGS and the Statement of Accounts.

The committee reviewed and formally **approved** the draft AGS and recommended that the S151 Officer have delegated authority to make minor amendments and changes.

8 Statement of Accounts (pre-audit training)

The Corporate Director Resources submitted a presentation along with a recording for the committee to review prior to the meeting.

She told the committee that prior to the pandemic, she would give this presentation during the meeting, however it was considered more efficient to provide the committee with a recording, which they could review at any time before the official Statement of Accounts was presented to the committee. She hoped the accounts would come to committee in July 2022, with the expectation the recorded presentation would support members in their discussion.

The recorded presentation was linked in the agenda pack, as well as being made available on the Councillor Portal.

9 Audit Progress 2020-21 and 2021-22 (including 2022-23 Audit Plan update)

Paul Hewitson, the external auditor from Deloitte, was in attendance at the meeting and presented the committee with the progress on the 2020/21 and 2021/22 audits.

He told the committee that the 2020/21 audit had been significantly delayed and that they were hoping to undertake a national prioritisation exercise to gain more resources and expertise on this with a view to getting through their local authority backlog over the summer of 2022. He said that they hoped to be in a position to start undertaking the final work on the 2020/21 audit over the summer with the hope of finalising it in September 2022.

He told the committee that one key national issue that needed to be resolved was the treatment of the infrastructure assets which for Wyre affected our sea defences. He said that there was a blanket ban on signing accounts with significant values in infrastructure assets and that they were awaiting determination for the correct accounting treatment from CIPFA. Once this had been resolved, they were hoping to move on to finalising the work.

For the 2021/22 audit, again they were focusing on addressing their backlog of local authority work, they hoped to start completing the work towards the end of 2022. He said that the external auditors had set themselves a final completion date for all local authority audit work on 31 March 2023, but were

also hoping to go into the new year with all current and delayed audit work completed.

He apologised to the committee for the delays in completing the audits. He explained that there was a chronic shortage of experienced auditors in the local authority sector. They were currently taking steps to address this.

Committee members asked questions of the external auditor on the issue of resourcing and around realistic dates for completion.

10 Audit scale fee for 2021-22 and 2022-23

Paul Hewitson, the external auditor, spoke to the committee regarding the scale fee for the 2021/22 and 2022/23 audit work.

He said to the committee that they were required to tell the committee the scale fee at the start of each audit year. The external auditors did not set their own fee, it was set by the Public Sector Audit Appointments Ltd. (PSAA). The set fee was to be £37,470 and any variation to that fee had to be agreed by the Corporate Director Resources (S151 Officer) and signed off by the PSAA.

He did however say that the work on the infrastructure assets could vary the fee, and that the fee had been set before changes to the Value for Money requirements as part of the new Code of Audit Practice, set by the National Audit Office. He however said that the newness of the VFM requirements meant that they would still complete the work and would agree any additional fees for this following completion when they would understand any impact better.

The committee thanked Mr Hewitson for his attendance at the meeting.

11 Time and date of the next meeting

It was agreed that the next meeting of the Audit Committee would be held on Tuesday 26 July 2022 at 6pm in the Council Chamber.

The meeting started at 6.01 pm and finished at 7.08 pm.

Date of Publication: 7 July 2022

Report of:	Meeting	Date
Mary Grimshaw, Legal Services Manager	Audit Committee	27 September 2022

Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)

1. Purpose of report

1.1 To provide an update following a recent inspection on RIPA by the Investigatory Powers Commissioner's Office (IPCO).

1.2 To approve a revised RIPA Policy.

2. Outcomes

2.1 Evidence that the council has complied with IPCO's recommendation following the inspection.

2.2 Demonstrates that the Council's policies and procedures are compliant with RIPA legislation.

3. Recommendations

3.1 To note the findings of the IPCO inspection report.

3.2. To approve a revised RIPA policy statement incorporating the recommendations made by the inspector and an external RIPA trainer.

4. Background

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

4.2 The Protection of Freedoms Act 2012 introduced a more restrictive

approach to the use of RIPA by local authorities by limiting the use of direct authorisations to serious crimes, i.e. those crimes punishable by a maximum custodial sentence of six months or more or those constituting an offence of selling alcohol or tobacco to children. The application must also have judicial approval by a magistrate before an authorisation takes effect and the magistrate needs to be satisfied that there are reasonable grounds for believing that the requirements of RIPA are met. The council has not used RIPA surveillance powers since 2012.

4.3 The council is required to have a RIPA policy. The current policy was last approved in November 2021 in compliance with the RIPA code of practice, which requires an annual review of the policy.

4.4 IPCO has taken over the inspection and oversight functions on RIPA, which was previously carried out by the Surveillance Commissioner's Office. The IPCO have confirmed that they will continue to ensure RIPA compliance by conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections when a Local Authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. The council's previous inspection was in 2019.

5. Key Issues and proposals

5.1 An IPCO inspector carried out a remote desktop review on 13 January 2022. Following the inspection a report was issued which can be summarised as follows:

- The inspector was satisfied with the RIPA arrangements in place and was satisfied that the council had demonstrated a level of compliance that removes, for the present, the requirement for an onsite inspection.

- The inspector commented that the RIPA Policy is comprehensive and well written. However the chapter on communications data required updating to reflect recent legislative changes. The committee should note that the council has not made any communications data authorisations.

- The inspector commented that it is pleasing to note that RIPA training continues to be delivered to relevant officers deployed in enforcement or regulatory services who are most likely to engage the powers. The most recent training was carried out on 6 January 2022.

- The inspector noted the helpful guidance in the RIPA Policy regarding the use of the internet and accessing social media. He also noted the action taken by council officers following the recent

training to capture the extent and scope of online activity.

- The inspector was satisfied that in accordance with paragraph 4.47 of the Home Office Covert Surveillance and Property Interference Code of Practice, the annual reporting requirements to the Audit Committee were sufficient to determine that the council's policy remains fit for purpose.

- The inspector explained that IPCO are undertaking a programme of work regarding how material acquired under RIPA is retained and they shared the data assurance letter with the council. As part of this process, the inspector examined the council's Data Protection Policy and Retention Schedules and found that they were in good order.

5.2 Following the recent training session which highlighted the use of social media in surveillance activities, the Head of Governance and Business Support has recently approached departmental heads to capture the extent and scope of online activity. Once this exercise is completed, all activity should be recorded and supervised, which will enable the Senior Responsible Officer to have confidence that such resources are being used in a controlled, auditable and well understood manner.

5.3 In light of the inspector's report, chapter 5 on communications data has been updated to reflect the legislative changes made by the Investigatory Powers Act 2016. Local authorities can now obtain details of in and out call data and cell site location for "applicable crimes". All Communications Data applications must now be processed through National Anti Fraud Network and will be considered for approval by the Independent Office of Communication Data Authorisation. There have also been other minor changes to the policy as suggested by the RIPA trainer. These changes can be seen as track changes in Appendix 1.

Financial and legal implications	
Finance	There are no direct financial implications associated with the changes. Training for staff, to ensure that they are kept up to date with good enforcement practices and revisions to RIPA, will be met from existing budgets.
Legal	The approval of the recommendations demonstrates that the council's policies and procedures are compliant with RIPA.

Other risks/implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There

are no significant implications arising directly from this report for those issues marked with an **X**.

risks/implications	**✓ / x**
community safety	x
equality and diversity	x
sustainability	x
health and safety	x

risks/implications	**✓ / x**
asset management	x
climate change	x
ICT	x
data protection	x

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a 3rd party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

report author	telephone no.	email	date
Mary Grimshaw	01253 887214	Mary.Grimshaw@wyre.gov.uk	15/09/2022

List of background papers:		
name of document	date	where available for inspection
None		

List of appendices

Appendix 1 - RIPA Policy Statement (with tracked changes)

The Regulation of Investigatory Powers Act 2000 (RIPA)

Policy Statement

To be approved by the Audit Committee 27 September 2022

Contents

Formatted Table

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates 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.

1.2 Wyre Borough Council is therefore included within the RIPA framework with regards to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources and access to Communications Data.

1.3 The purpose of this guidance is to:-

- explain the scope of RIPA and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed

1.4 The council has had regard to the Codes of practice produced by the Home Office in preparing this guidance and copies are attached at Appendix 4.

1.5 In summary, RIPA requires that when the 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 is satisfied. Following changes made by the Protection of Freedoms Act 2012 all authorisations must be approved by a magistrate. If an officer requires access to communications data, the framework is provided by the Investigatory Powers Act 2016, and associated codes of practice. The authority must make the application through NAFN, the National Anti-Fraud Network, who by virtue of a collaborative agreement act as the authority SPOC. An extract from the Scheme of Delegation indicating the Authorising Officers is attached at Appendix 2.

Formatted: Font: (Default) Arial, Font color: Red

Formatted: Font: Bahnschrift SemiBold, Font color: Red

Formatted: Font color: Red

1.6 Authorisation under RIPA gives lawful authority to carry out directed surveillance and the use of covert human intelligence source. Obtaining authorisation helps to protect the council and its officers from complaints of interference with the rights protected by Article 8 (1) of the European Convention on Human Rights and the UK which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law", and for a legitimate purpose. Provided activities undertaken are also "reasonable and proportionate" they will not be in contravention of Human Rights Legislation.

Formatted: Indent: Left: -0.14 cm, Hanging: 0.5 cm

1.7 Authorising Officers and Investigators within the Local Authority are to note that RIPA does not extend powers to conduct intrusive Surveillance. Investigators should familiarise themselves with the provisions of the Code Of Practice on Directed Surveillance and Covert Human Intelligence Sources to ensure a good understanding of the limitation of powers within RIPA. Deciding when authorisation is required involves making a judgement. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Senior Responsible Officer.

2 Directed Surveillance

2.1 **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.

2.2 **When is surveillance directed?**

Surveillance is 'Directed' for the purposes of RIPA if it is covert, but not Intrusive and is undertaken:

a) for the purpose 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 one is specifically identified for the purpose of the investigation or operation); and

c) otherwise than by the way of an immediate response to levels 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.

2.3 **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'',** 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 carrying out by any 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, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtain from a device actually present on the premises or in the vehicle.

It should be noted that the council cannot authorise "intrusive surveillance''

2.4 Before any officer of the council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within RIPA. In order to do this the following key questions need to be

asked.

2.4.1 **Is the surveillance covert?**

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the RIPA framework does not apply.

Examples of the surveillance are provided in the Code of Practice and are summarised in Appendix 3.

2.4.2 ***Is* it for the specific investigation or a specific operation?**

If officers are monitoring general activity in a street or car park whether covert or overt, then it is not covered by RIPA, as such general observation duties are part of the legislative functions of public authorities and are not pre-planned surveillance of a specific person or group of people.

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

"Private information" is any information relating to a person's Private life or family life.

It is an issue of fact and degree, which has to be examined in each case.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that persons' activities 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 the future consideration.

Example:
Officers of a local authority wish to drive past a café for the purpose of taking a photograph of the exterior. This is not likely to require a directed surveillance authorisation, as no private information about any person is likely to be obtained. However if the authority wish to establish a pattern of occupancy of the premises, the accumulation of information is likely to result in the obtaining of private information and a direct surveillance authorisation should be considered.

If it is likely that observation will not result in the obtaining of private information about a person, then it is outside RIPA.

2.4.4 **Otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation**

An example of an immediate response to something happening during the course of an observer's work which is unforeseeable would be a housing benefit fraud officer who conceals himself and continues to observe a person working who he knows to be claiming benefits and whom he comes across unexpectedly.

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

2.4.5 **Surveillance – Direct or Intrusive?**

Directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not in the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as it if were.

Commercial premise and commercial vehicles are therefore excluded from intrusive surveillance.

High quality video monitoring or CCTV may run a significant risk of providing consistently high quality data "as if you were there" and therefore come within the definition of intrusive surveillance.

Matron boxes i.e. noise monitors, used by environmental health departments will not usually be covered. Usually they are stationed in a neighbouring property and do not provide evidence of the same quality as if the device was actually on the premises. Also the code of practice advises that in such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy.

The council is not authorised to carry out intrusive surveillance.

3 Covert use of Human Intelligence Source (CHIS)

3.1 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.

3.2 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 that purpose.

3.3 A relationship is used covertly and an information obtained is disclosed covertly, if and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

3.4 An example by the Home Office is where intelligence suggests a local shop keeper is selling alcohol to underage customers and the local authority engages an employee to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited, that the authority can conclude that an authorisation is unnecessary.

3.5 **Lay Witness**

Choose carefully how you chose to ask lay witnesses to gather information for you. For example, if a member of the public telephones to complain about noise nuisance caused by a neighbour. The lay witness is in a relationship with the neighbour already and is just passing on information to the council and would not be covered by RIPA. However the more the council tasks the lay witness to do something then you may inadvertently change them into a CHIS.

If you are in doubt seek advice from a senior Authorising Officer, and if they are in doubt they will seek advice from a Senior Responsible Officer.

3.6 **The use of Covert Human Intelligence Sources**

3.6.1 In practice it is most unlikely that it will ever be appropriate for the council to utilise a CHIS. However, in the event that it is ever considered, advice should be sought from the Senior Responsible Officer at an early stage. It is potentially possible that a council employee may be that of a source or the council may also use an external or professional source for the

purpose of obtaining information. Such persons may be a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b or c of paragraph 3.1.

3.6.2 Nothing in RIPA prevents material obtained by an employee acting as a source being used as evidence in court proceedings.

3.6.3 The Authorising officer must consider the safety and welfare of a CHIS acting a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given and considering what issues could be facing the security and welfare of a CHIS in relation to what they are being asked to do. This should take place before authorisation is granted, at any renewal, review and cancellation.

3.6.4 Before authorising the use of a CHIS as a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion) Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

3.6.5 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, "confidential material" is likely to be obtained. (see definition of confidential material in Appendix 1) Special provisions relate to vulnerable individuals and juvenile services.

3.6.6 In additional to the usual authorisation process, the following management arrangements must be in place at all times in relation to the use of a CHIS:

1. There will be an appropriate officer of the council (handler) who has day-to-day responsibility for dealing with the CHIS, and for the security an welfare of the CHIS; and

2. there will be a second appropriate officer of the council who has general oversight of the use made of the CHIS, and who will have responsibility for maintaining an accurate and proper record about the source and tasks undertake (~~manager and recorder~~ controller or covert manager)

3.6.7 The CHIS forms contain appropriate boxes and prompts for ensuring the above is carried out.

4 Duration, Authorisations, Reviews Renewals and Cancellations

4.1 Duration

4.1.1 Authorisations lapse, if not renewed

4.1.1.1 within 12 months - from date of last renewal if it is for the conduct or use of a covert human intelligence source or;

4.1.1.2 in all other cases (i.e. directed surveillance) 3 months from the date of their grant or last renewal.

4.1.2 Directed Surveillance - Authorisation

4.1.2.1 For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

a. that an authorisation is **necessary** (on the one the ground detailed below) and

b. the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

4.1.2.2 An authorisation is necessary on the grounds stated below following the introduction of the Protection of Freedoms Act 2012:-

a. for the purpose of preventing or detecting conduct which constitutes/corresponds to a criminal offence that is punishable by a maximum custodial sentence of 6 months or more or;

b. constitutes an offence under s.146, 147or 147A of the Licensing Act 2003) - selling alcohol to children or;

c. selling tobacco to persons under 18 years of age (s.7 Children and Young Persons Act 1933).

4.1.2.3 The Authorising Officer should be set out, in its own words, why he believes the activity is necessary and proportionate. A bare assertion is insufficient. The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

a. necessary for the ground stated above and be able to demonstrate the reasons why it is necessary and;

b. proportionate to its aim.

This involves balancing the seriousness of intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an

expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

The following elements of proportionally should therefore be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- Explaining how and why the methods will cause the least possible intrusion on the subject and others;

- Considering whether the activity is an appropriate use of the legislation and a reasonable way having considered all reasonable alternatives of obtaining the necessary result;

- Evidencing as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all officers involved in surveillance are fully aware of the extent and limits of the authorisation.

The Code of Practice give an example of an individual suspected of carrying out a series of criminal damage offences at a local shop after a dispute with the owner. It suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purpose of preventing or detecting crime. Although these are legitimate grounds on which directed surveillance may be conducted, the Home Office Code states that it is unlikely the interference with privacy will be proportionate in the circumstances of the particular case. In particular the obtaining of private information on the individuals daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.

4.1.2.4 In order to ensure Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained. The applicant in completing the forms must provide facts and evidence.

4.1.2.5 It is also sensible to make any authorisation sufficiently wide enough to cover the means required as well as being able to prove effective monitoring of what is done against what is authorised.
Authorisations must be in writing. The standard forms to be used can be accessed via the council's intranet.

4.1.2.6 **IMPORTANT NOTE: THE PROTECTION OF FREEDOMS ACT 2012 INTRODUCES A REQUIREMENT FOR MAGISTRATE APPROVAL FOR ALL RIPA AUTHORISATIONS FROM 1 NOVEMVER 2012. ACCORDINGLY AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A JP HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL.**

The procedure and application process is set out in Appendix 8. It is important that you seek advice from the Senior Responsible Officer before making the application for judicial approval.

4.1.2.7 Any Authorising officer proposing to approve an application for the use of directed surveillance, or for the use of CHIS must immediately inform the Senior Responsible Officer, who will then make arrangements for an application to be made to the Magistrates' Court.

4.1.2.8 In such circumstances the council will be required to make an application, without giving notice to the Magistrates Court. The Magistrates will give approval if and only if, at the date of the grant of authorisation or renewal of an existing authorisation they are satisfied that:

a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these ground still remain

b) the "relevant conditions" were satisfied in relation to the authorisation.

Relevant conditions include that:

1. the relevant person was a designated as an Authorising Officer.

2. it was reasonable and proportionate to believe that using covert surveillance or a CHIS was necessary and that the relevant conditions have been complied with.

3. the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25 (3) of RIPA (restrictions on the rank of the person granting the authorisation)

4. any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant or renewal of the authorisation, it may make an order to quash that authorisation. However the court may not exercise its power to quash the authorisation unless the council has had at least two business days from the date of refusal in which to make any representations.

4.1.3 **Reviews**

4.1.3.1 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

4.1.3.2 It is recommended that regular reviews be undertaken to see if the need for the surveillance is still continuing. Results of reviews should be recorded in the Central Register of Authorisations (see paragraph 7) Reviews should be more frequent when access is more confidential information or collateral intrusion is involved. Review frequency should be

as often as the Authorising Officer deems necessary or practicable.

4.1.3.3 Each Authorising Officer will therefore determine in each case how often authorisations should be reviewed. It is recommended that they ensure records of the review be supplied on the relevant form. Copies should be sent to the Senior Responsible Officer to keep the Central Register up to date.

4.1.4 **Renewals**

4.1.4.1 An Authorising Officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. A renewal of the authorisation in writing can be made for up to 3 months. Applications for renewal should detail how any times an authorisation has been renewed; significant changes to the original application for authority; reasons why it is necessary to renew; content, value of the information obtained so far and results of regular reviews of the investigation or operation.

4.1.4.2 Each application to renew should be made at least 7 days before the authorisation is due to expire on the relevant form. A record of the renewal should be kept within the applying service and supplied centrally to the Senior Responsible Officer to be placed in the Central Register.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 RENEWALS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE RENEWAL.

4.1.5 **Cancellations**

4.1.5.1 All Authorisations, including renewals should be cancelled if the need for surveillance is no longer justified. This will occur in most cases where the purpose for which the surveillance was required has been achieved.

4.1.5.2 Requesting officers should ensure they inform authorising officers if this is the case before the next review. If, in opinion of the Authorising Officer at the next review the need for surveillance is no longer justified it must be cancelled.

4.1.5.3 The cancellation forms will be used to record a cancellation, and the Authorising Officer will ensure the original cancellation has been sent to the Senior Responsible Officer or nominated reprehensive to update the Central Register.

4.2 **Covert use of Human Intelligence Sources**

4.2.1 **Authorisation**

4.2.1.1 The same principles as set out in paragraphs 4.1.2.1 and 4.1.2.2 apply to CHIS except the ground on which a CHIS can be authorised, which remains unaltered by the Protection of Freedoms Act 2012.

A CHIS authorisation can only be approved where it is necessary for the purpose of preventing or detecting crime, or preventing disorder.

A CHIS authorisation can last for up to 12 months.

4.2.1.2 The conduct so authorised is any conduct that:

a) is comprised in any such activities involving the conduct or use of a ~~covert human intelligence source~~CHIS, as are specified or described in the authorisation;

b) relates to the person who is specified or described as the person whose actions as a ~~covert human intelligence source~~CHIS the authorisation relates; and

c) is carried out for the purpose of, or in connection with the investigation or operation so specified or described.

4.2.1.3 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against the authorised.

4.2.2 ***Renewals/Reviews***

4.2.2.1 Similar provisions apply for a CHIS except that a renewal here can last for a further 12 months, a review must have been carried out on the use of the source and an application should only be made to renew when the initial authorisation period is drawing to an end. Applications to renew a CHIS also should contain use made of the source and tasks given to the source during the previous authorised period and the information obtained.

IMPORTAMT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E A GRANT OR RENEWAL.

4.2.3 **Cancellations**

4.2.3.1 The same principles as Directed Surveillance apply.

4.2.3.2 Separate forms have been devised to applications to authorise, review, renew and cancel a CHIS. These can be accessed via the Councils intranet.

5 Communications Data

~~5.1~~ ~~**Acquisition of Communications Data**~~

5.1 Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer.

5.2 Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

5.3 Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

5.4 A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice.

5.5 Finally, the IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

~~The Regulation of Investigatory Powers (Communications Data) Order 2010 replaced the earlier 2003 order which gave local authorities the powers set out within RIPA to access communications data. The 2010 Order raised the seniority of the Authorising Officers in local authorities to a Director, Head of service, Manager or equivalent.' Communications data~~

Formatted: Indent: Left: 2 cm

~~includes information relating to the use of a communications service but it does not in include the contents of the communications itself. Communications data can be split into three types; "traffic data" i.e. where a communication was made from, to whom and when; "service data" is the use made by the service by any person eg itemised telephone records; and "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to. Local authorities are allowed to access "service data" and "subscriber data"; they are not allowed to access "traffic data".~~

~~5.2~~ ~~**Authorisation**~~

~~The Order permits access to communications data, by local authorities only where it is necessary for the purpose of preventing or of detecting crime or preventing disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve. It should not be authorised where less intrusive means can be used to further an investigation~~

~~5.3~~ ~~**Alternative methods for authorisation**~~

~~Access to communications data may be authorised in two ways; either (a) through an authorisation by an Authorising Officer which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data provided it to the local authority.~~

~~5.4~~ ~~**Application**~~

~~Application will be made by the investigating officer and submitted to a Single Point of Contact (SPOC) who will either accept or reject the application. If the SPOC accepts the application he will forward it together with a SPOC report and a draft notice (where appropriate) to an Authorising Officer for authorisation.~~

~~If the Authorising Officer accepts the application, it will need to be approved by a magistrate before the forms are returned to the SPOC and the SPOC will deal with the postal or telecommunications operator directly. The SPOC will also advise investigating officers and Authorising Officers on whether an authorisation or notice is appropriate in the circumstances.~~

~~Although it's unlikely that the Council will access communications data, in the event that it did, the Council would appoint a nominated SPOC and NAFN, (National Anti-Fraud Network) who have received training on a course recognised by the Home Office.~~

~~**Authorising officers**~~

~~Authorising Officers for the purpose of communications data will be the same as for directed surveillance and CHIS's~~

Formatted: Indent: Left: 0 cm

Formatted: Indent: Left: 0 cm

Formatted: Indent: Left: 0 cm

Formatted: Indent: Left: 1.27 cm

~~IMPORTANT NOTE: FROM 1NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION. SEE PARAGRAPHS 4.1.2.6 – 4.1.2.8 ABOVE~~

Formatted: Indent: Left: 1.27 cm, First line: 0 cm

6 Other factors to consider

Particular consideration should be given to **collateral intrusion** i.e. the risk of intrusion into the privacy of those not directly the targets of the investigation. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality test, as outlined above apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject if the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

6.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the surveillance.

6.3 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subject of the investigation or covered by an authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

6.4 Any person giving authorisation will also need to be aware of 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.

Confidential Material

6.5 RIPA does not provide any special protection for **"confidential material"** (see definitions in Appendix 1) Nevertheless, such material is particularly sensitive, and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to a special authorisation. i.e. by the Chief Executive.

6.6 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken when the target of the investigation is likely to be involved

in handling confidential material. Such applications should only be considered in the exceptional and compelling circumstances with full regard to the proportionality issues this raises.

6.7 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be altered to anything that may fall within the definition of confidential material where there is doubt as to whether the material is confidential, advice should be sought from the Senior Responsible Officer before further dissemination takes place;
- Confidential material should not be retained or copied unless it is necessary for a specific purpose;
- Confidential material should be disseminated only where an appropriate officer (having sought advice from the Senior Responsible Officer) is satisfied that it is necessary for a specific 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.
- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

6.8 In the case of confidential information a higher level of authorisation is Required. Therefore where authorisation is sought to carry out surveillance in respect in respect of communications subject to legal professional privilege, or containing confidential personal information or confidential journalistic material, the Chief Executive must sign the authorisation.

Joint Working

6.9 In cases of joint working, where one agency is acting on behalf of another, usually the tasking agency can obtain or provide the authorisation i.e. if the Council has been tasked by the Police to assist in a covert surveillance operation, they should get the authorisation, which would the cover the Council. But advice should be sought from the Senior Responsible Officer prior to any arrangements being agreed.

Handling and Disclosure of Materials

6.10 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 6.7

above.

6.11 Applications and associated reviews, renewals and cancellations for directed surveillance shall be centrally retrievable for a period of 5 years Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

6.12 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject if 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 is whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer. If in doubt advice should be sought from the Senior Responsible Officer.

6.13 There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However the use outside the Council, of any material obtained by means of covert surveillance and other than in pursuance of the ground, on which is was obtained, should be authorised only in the most exceptional circumstances. Advice should be sought from the Senior Responsible Officer.

7 Central Register of Authorisation

7.1 The RIPA code of practice requires a central register of all authorisations to be maintained. The Legal Section maintains this register.

7.2 Whenever an authorisation is authorised, renewed, reviewed or cancelled the Authorising Officer must send the signed original authorisation to the Senior Responsible Officer or nominated representative. Receipt is the form will be acknowledged.

7.3 The Central Register will contain the following information:

- the type and date of authorisation;
- the name and grade of the Authorising Officer;
- a unique reference number for the investigation or operation;
- the title of the investigation/operation, and a brief description and names of the subjects, if known;
- if an authorisation is renewed, when and the name and designation of the Authorising Officer;
- if confidential information is likely to be a consequence of the investigation or operation;
- the date the authorisation was cancelled;
- the date of magistrates court approval.

7.4 The legal section will securely retain the original authorisations and maintain the Central register. Authorisations should only be kept for a

maximum of 5 years from the end of an authorisation. Once the investigation is closed (bearing in mind cases may be lodged sometime after the initial work) the records held by the department should be disposed of in an appropriate manner (e.g. Shredded)

8 Codes of Practice

8.1 There are Home Office codes of practice and Office of Surveillance Commissioners (OSC) Guidance that expand on this policy statement and copies are attached at Appendices 4 and 6. The codes also list General Best Practices, which should be followed where at all possible.

8.2 The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account''

8.3 Staff should refer and familiarise themselves with the Home Office Code of Practice and OSC Guidance for supplementary guidance.

8.4 Authorising Officers and the Senior Responsible Officer should also familiarise themselves with the Procedures and Guidance document produced by the OSC attached at Appendix 6.

9 Benefits of obtaining Authorisation under RIPA

9.1 **Authorisation of surveillance and human intelligence sources**

RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and;
- the conduct is in accordance with the authorisation, then;
- "it shall be lawful for all purposes"

However, the corollary is not true – i.e. if you do not obtain RIPA authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means that you cannot take advantage of any of the special RIPA benefits.

9.2 RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which:

a) is incidental to any conduct that is lawful by virtue of an authorisation and;

b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

10 Scrutiny and Tribunal

10.1 The Investigatory Powers Commissioners Officer (IPCO) has taken over the inspection and oversight functions on RIPA which was previously carried out by the Surveillance Commissioner's Office. The IPCO and his assistants will continue to ensure RIPA compliance by conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections what a local authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. However, a desktop inspection will always be followed by an onsite inspection.

10.2 RIPA provides for the establishment of a tribunal to consider and determine complaints made under RIPA, and persons aggrieved by a local authority's conduct e.g. directed surveillance can make complaints to the tribunal. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

10.3 The tribunal can order, among other things, the quashing or cancellation of any authorisation and can order destruction of any records or information obtained by such authorisation, and records of information held by any public authority in relation to any person. The council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A council Officer has granted any authorisation under RIPA.
- Council employees have engaged in any/all conduct as a result of such authorisation.
- A disclosure notice requirement is given.

11 Covert Surveillance of Social Networking Sites (SNS)

11.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist it in preventing or detecting crime or carrying out any other statutory functions, as well as understanding and engaging with the public is serves. It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be assessed without the need for RIPA authorisation (use of the internet prior to an investigation should not normally engage privacy considerations)

11.2 If the study of an individual's online presence becomes persistent or where material obtained from any check is to be extracted and recorded any may engage privacy considerations, RIPA authorisations many need to be considered.

11.3 Officers are required to follow the processes outlined in Appendix 11,

when viewing social media sites in investigations or to gather information.

11.4 The following guidance taken from the Home Office Covert Surveillance and Property Interface Revised Code Of Practice (August 2018) is intended to assist the council in identifying when such authorisations may be appropriate.

11.5 The internet may be used for intelligence gathering and/or as a surveillance tool.

11.6 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group and authorisation for directed surveillance should be considered, as set out elsewhere in this policy

11.7 Where an officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed. However, it is considered that it is most unlikely that it will ever be appropriate for the council to utilise a CHIS.

11.8 In deciding whether online surveillance should be regarded a covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or maybe taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where the council has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be required.

11.9 Depending on the nature of online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain. However in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

11.10 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by the council of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hole a reasonable expectation of privacy in relation to the information.

11.11 Whether the council interferes with a person's private life includes a consideration of the nature of the councils activity in relation to that

information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) it's unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a council is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

Example 1:
An officer undertakes a simple internet source on a name address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation. authorisation should then be considered.

Example 2:
An officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought)

Example 3:
An officer undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends possible indicators or criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation, however when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation authorisation should be considered.

11.12 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake factors that should be considered in establishing whether a directed surveillance authorisation is required to include:

- Whether the investigation or research is directed towards an

individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide and observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, many still require a directed surveillance authorisation.
- Intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties;
- Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

Example:
Officers using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

12 Conclusion

12.1 If you can carry out investigations in an obviously overt way so that it does not compromise what you are trying to achieve then you need to consider RIPA and you are advised to take a broad view and interpretation of your activities. If you are in doubt you can seek advice from the Senior Responsible Officer and remember if there is any doubt then it is usually safer to get authorisation.

APPENDIX 1

Definitions from the 2000 Act

- "**RIPA"** means the Regulation of Investigatory Powers Act 2000.
- "SRO" means Senior Responsible Officer
- "CHIS" means Covert Human Intelligence Sources
- "**Confidential material"** consists of:

  a) Matters subject to legal privilege;

  b) Confidential personal information; or

  c) Confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A Below).

- **"Confidential personal information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or mental health or;

  b) to spiritual counselling or other assistance given, and;

which a person has acquired or created in the course of any trade, business profession or other occupation or for the purpose of any paid or unpaid office (see Note B below) it includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  c) it is held subject to an express or implied undertaking to hold it in confidence, or;

  d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- **"Confidential Journalistic Material"** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purpose of journalism and held subject to such an undertaking.

- **"covert Surveillance**" means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

- **"Authorising Officer"** means a person designated for the purpose of RIPA to grant authorisations for directed surveillance.

Note A *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal advisor is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal advisor is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation*

Note B *Confidential personal information might for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

APPENDIX 2

Extract from Part 7 of the Councils Constitution - Management Structure and Scheme of Delegation

Scheme of Delegation to Officers -

All delegations to officers are subject to the following general conditions:

(2) In the absence of the Chief Executive the functions of the Chief Executive will be the responsibility of any of the Corporate Directors. ~~either one of the three Services Directors~~

Formatted: Indent: Left: 1.88 cm, Hanging: 0.12 cm

Executive functions Delegated to the Chief Executive (8~~7~~) To Provide the necessary authorisations in respect of surveillance in accordance with the Regulation of Investigatory Powers Act 2000, where confidential information is involved or where authorisation is sought for the employment of a juvenile or vulnerable Covert Human Intelligence Source (CHIS).

Executive Functions Delegated to the ~~Service~~ Corporate Directors

(2) To act as authorising officers for the purpose of the Regulation of Investigatory Powers Act 2000 and Protection of Freedoms Act 2012.

Executive Functions Delegated to the Legal Services Manager

(3) To act as the Senior Responsible Officer for the purpose of Part ll of the Regulation of Investigatory Powers Act 2000.

(5~~4~~) To make an application to a justice of the Peace in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application.

Executive Functions Delegated to Revenues Manager and Senior Compliance Officers~~Fraud and Compliance Manager and Fraud Investigation Officers~~

(1) To make an application to a justice of the Peace, in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the council in making such an application.

(3) Power to carry to carry out surveillance which is governed by the Regulation of Investigatory Powers Act 2000 as agreed by an authorising officer.

APPENDIX 3

Examples of Surveillance

Examples of different types of surveillance	**Examples**
Surveillance that does **not** require RIPA Authorisation.	- Council Officers on patrol who conceal themselves to observe suspicious persons that they come across in the course of a routine patrol. - Signposted Town Centre CCTV cameras (in normal use) -Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Sampling purchases (where the officer behaves no differently from a normal member of the public) - Dog warden in uniform on patrol on park, street or van. - Food Safety or Health and Safety Inspections. -General observational duties not specifically targeted/planned or considered direct surveillance. - CCTV cameras providing general traffic, crime or public safety information. - Covert surveillance of an employee who is suspected by his employer of undertaking additional duties in breach of discipline regulations, as it does not relate to the discharge of the Employers core functions.
Covert directed Surveillance must be RIPA authorised	Officers follow/observe an individual or individuals over a period, to establish whether s/he is working when claiming benefit provided the conduct constitutes/corresponds to a criminal offence punishable with at least 6 months imprisonment.
Surveillance that is not intrusive.	**-** An observation post outside residential premises, which provides a limited view compared to that which would be achievable from within the premises.
Intrusive - **Council cannot do this!**	- Planting a listening or other device in a person's home or in their private vehicle - use of a zoom lens outside residential premises, which consistently archives imagery of the same quality as that which would be visible from within the premises.

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	27 September 2022

ANNUAL REVIEW OF THE COUNCIL'S RISK MANAGEMENT POLICY

1. Purpose of report

1.1 To review and approve the council's refreshed Risk Management Policy following the roll out of new risk management software and the delivery of risk management training across the council.

2. Outcomes

2.1 Evidence that the council manages its significant business risks and recognises that effective risk management is integral to the council's corporate governance arrangements.

3. Recommendation

3.1 That the Audit Committee reviews and approves the refreshed Risk Management Policy attached at Appendix 1.

4. Background

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

4.2 In accordance with their terms of reference, the Audit Committee will review the risk profile of the organisation and consider the effectiveness of the council's risk management arrangements. This involves monitoring the progress of embedding risk management, reviewing the council's risk registers/reports and ensuring that actions are being taken where necessary to mitigate such risks.

4.3 The Audit Committee review the Risk Management Policy on an annual basis, the next review of this policy being due in September 2023.

4.4 Since the last review in November 2021, the council has rolled out the new GRACE (Governance, Risk and Control Evaluation) risk management software and has delivered one-to-one risk management training to over 20 members of staff (Directors, Heads of Service and Service Managers) to assist with the embedding of risk across the organisation.

4.5 Whilst Audit Committee will not have direct access to GRACE, reports for both strategic and operational risks will be produced and uploaded to the HUB on a quarterly basis.

5. Key Issues and proposals

5.1 The refreshed Risk Management Policy is at Appendix 1. The Policy, in particular Section 7, has been amended following its last review in November 2021 to reflect some procedural changes following the roll out of GRACE and the 'switching on' of the email notification function. A new section has also been added at Section 10 to set out how the risk management process will link with the internal audit process and the following-up of audit recommendations.

Financial and legal implications	
Finance	None arising directly from the report.
Legal	Effective risk management assist in good governance and probity of council actions.

Other risks / implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

risks/implications	**✓ / x**
community safety	x
equality and diversity	x
sustainability	x
health and safety	x

risks/implications	**✓ / x**
asset management	x
climate change	x
ICT	x
data protection	x

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a third party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

report author	telephone no.	email	date
Dawn Allen	01253 887341	dawn.allen@wyre.gov.uk	14 August 2022

List of background papers:		
name of document	date	where available for inspection
None		

List of appendices

Appendix 1 – Risk Management Policy (refreshed August 2022)

This page is intentionally left blank

Risk Management Policy

Wyre Borough Council
Risk Management Policy V2.0
To be approved by Audit Committee - 27 September 2022

Contents

Version control

	Description	Date
V0.1	Draft Risk Management Policy	14/10/21
V0.2	Draft Risk Management Policy to Audit Committee	16/11/21
V1.0	Approved by Audit Committee	16/11/21
V1.1	Review of Risk Management Policy	01/08/22
V1.2	Draft Risk Management Policy to Audit Committee	27/09/22
V2.0	Approved by Audit Committee	

1.0 Introduction

1.1 Risk is unavoidable and is part of life. As an organisation, we need to take risks to grow and develop. Risk management involves understanding, analysing and addressing risks to make sure that 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 robust corporate governance supporting the effective use of the council's resources, as well as improved decision making and budgeting, and enhanced communication between staff, elected members and partners.

1.2 This policy explains the 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.

1.3 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.

2.0 Scope

2.1 This policy applies to all staff, 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 within this policy.

2.2 This policy will be reviewed annually to take account of changing legislation, government initiatives, best practice, changes to internal procedures 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. 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 any 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 Definitions

4.1 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."

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

Strategic Risks – Risks that could have an effect on the successful achievement of the Council's long term vision, business plan 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 plans/objectives. Potentially these risks could have a significant financial, reputational and/or service delivery impact on the business unit as a whole.

5.0 Risk Management Standards

5.1 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.

5.2 Despite the publication of the global risk management standard in 2009; ISO 31000 (updated early 2018), 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.

5.3 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.

6.0 Risk Management Approach

6.1 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.

6.2 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 business plan, individual services plans, project briefs, partnership agreements etc.

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

Step 1 – Identifying risk

6.4 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 or 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;
- officers/Elected Members 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.

6.5 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.

6.6 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 Checklist for Risk Identification at **Appendix A**.

6.7 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.

6.8 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

6.9 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.

6.10 To ensure that a consistent scoring mechanism is in place across the council, risks are assessed using agreed criteria for likelihood and impact and a score is calculated using the risk matrix e.g. High Likelihood (3) and High Impact (3) would result in a risk score of 9 – see **Appendix B**.

6.11 A "traffic light" approach is used to show high (red), medium (amber) and low (green) risks.

First Risk Score – Inherent (Gross) Risk Score

6.12 Following identification of the risk, a score for the gross likelihood and gross impact will be given to the risk as it currently stands, to ascertain the inherent (gross) risk score. The inherent risk score is the score given before any controls or actions are taken to alter the risk's impact or likelihood. This risk score is given to assist Internal Audit when pulling together the Risk Based Audit Plan. Those risks that have scored as 'red' risks will be the risks that Internal Audit will want to ensure are appropriately mitigated and will therefore take priority when the audit plan is produced.

Second Risk Score – Residual (Net) Risk Score

6.13 Risks are then re-scored to ascertain the residual (net) risk score. This is the score given when taking into consideration any controls already in place and/or any existing actions that are not operating effectively. To ensure resources are focused on the most significant risks, the council's approach is to focus on the risks that have scored as 'red' or 'amber' on the matrix. This may also be referred to as the council's risk appetite. The residual risk score will be the deciding factor as to whether further action is required in order to reduce the risk to within the council's 'risk appetite'. It is at this point that a risk response category is assigned by the risk owner to determine what, if any, action is to be taken e.g. reduce or accept the level of risk. (**See Appendix C for risk response categories.**)

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

Third Risk Score – Target Risk (Retained Risk) Score

6.15 If a risk requires further mitigating action in order to reduce the risk score to within a tolerable level, the risk owner needs to set a realistic target score, and develop an action plan which when implemented will reduce the risk to within the target risk score.

Step 3: Treatment and Action Planning

6.16 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.

6.17 Residual risks are prioritised by applying the same scoring criteria and matrix used for assessing the Inherent risk level (Step 2). It is the risk owner's responsibility to ensure that the agreed residual risk level for each risk is an accurate reflection of the likelihood and impact measures detailed in **Appendix B.** Where the severity of a risk is reduced, evidence of the mitigating action taken in the implementation of the activity being assessed should be retained.

6.18 Not all risks can be managed, 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, the following ways:

- **Terminate** - A decision is made not to take a risk;
- **Tolerate** - A decision is taken to accept the risk;
- **Transfer** - All or part of the risk is transferred through insurance or to a third party;
- **Treat** - 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.

6.19 These actions are described in more detail in **Appendix C.**

6.20 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

6.21 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.

6.22 Regular reporting enables senior managers and Elected Members to be more fully aware of the extent of the risks and progression being made to manage them. Both strategic and operational risk workshops will be administered by Internal Audit on an annual basis.

6.23 The GRACE Risk Management system encourages risk owners to continually monitor and update identified risks through the automatic email reminder function.

The system automatically generates and sends an email every Monday morning to all officers that have overdue risk actions within their registers, requesting them to review and update them.

6.24 In addition, quarterly email notifications are sent to risk owners asking them to consider/add newly identified risks to the system and review current risks, scores and action plans.

6.25 Progress on high 'red' risks for both strategic and operational risk registers will be reported to the Audit Committee as required.

7.0 Risk Registers

7.1 The council's risk registers are held within the GRACE Risk Management system. The registers document the key risks and who is responsible for them. It also records the action plans created to help mitigate these risks.

7.2 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.

7.3 The Audit and Risk Team will oversee the administration of both strategic and operational risk registers within the GRACE system. However, identified risk owners will ultimately be responsible for monitoring and updating their risk scores and actions plans.

7.4 The GRACE system will automatically send risk owners a weekly email notification detailing overdue actions within their risk registers and a quarterly risk review notification to all risk owners. Internal Audit will monitor risk movements to ensure that risk/action owners are updating records as and when required.

7.5 Managers are encouraged to amend risk scores or descriptions with the intention of maintaining a culture of openness. However, Internal Audit will monitor these amendments to ensure that actions taken e.g. increased or improved control, or another viable explanation e.g. the activity ceases altogether, has been recorded within the system to support the change.

8.0 Roles and Responsibilities

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

8.1.1 Employees

- Manage day to day risks and opportunities effectively and report risk management concerns to their Heads of Service/Mangers;
- Participate fully in risk workshops and action planning as appropriate and;
- Attend training and awareness sessions as appropriate.

8.1.2 Elected 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.

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

8.1.3 Cabinet

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

8.1.4 Audit Committee

- Provide independent assurance to the council on the overall adequacy of the risk management framework, including a review of proposed amendments to the Risk Management Policy;
- 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.

8.1.5 Corporate Management Team

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

8.1.6 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 Corporate Director Resources (Section 151 Officer), supported by the Audit and Risk Manager (Chief Internal Auditor), champion 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.

8.1.7 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 the 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 Statement review process.

8.1.8 Risk Owners

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

8.1.9 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.

8.1.10 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 Corporate Management 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.

9.0 Embedding Risk Management

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

10.0 Risk Management and the Audit Process

10.1 All agreed actions resulting from Internal Audit reviews will be added to the audit area of the GRACE risk management system (not within individual operational risk registers). The HOS or Service Manager of the audited area will be recorded as the action owner alongside the Auditor who carried out the review. This will ensure that all actions are monitored and reviewed in the same way as the strategic and operational risks, through the receipt of weekly 'overdue' reminder notifications.

10.2 All audits receiving a 'Substantial' or 'Reasonable' assurance opinion will be informally followed-up. This means that action owners will be prompted through the automated email notification process to update the audit actions within GRACE and the Internal Audit Team will review GRACE to ensure that all outstanding actions are completed to a satisfactory level, but reliance will be placed on the action owner's update.

10.3 However, audits receiving a ‘Limited’ or ‘Minimal/No’ assurance opinion will be formally followed up six months after the original audit report was issued (a diary date will be added to the Auditor’s Outlook calendar to prompt this). A review of the risk actions in GRACE will be undertaken, testing will be carried out as required and a follow-up report will be issued with a second audit assurance opinion. Again the GRACE system will prompt action owners to address their actions through the automated email notification process as and when risk actions become overdue.

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 staff and Elected Members with the knowledge and skills necessary to enable them to manage risk effectively. Internal Audit will use a range of training methods to meet the needs of the organisation. Furthermore, risk management information will be developed and will be made 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 A

Checklist for Risk Identification (PERFORMANCE)

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 and 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 / external funding
- Effects of the change in central government policies
- Exposure to regulators (auditors/inspectors)
- 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 Wyre 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, cyber 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

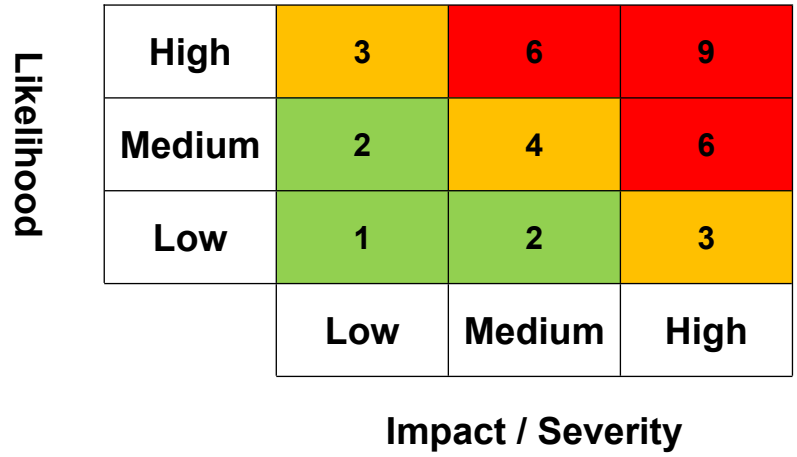
Environment

- 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 and drier summers, milder and wetter winters and more extreme events – heatwaves, flooding, storms etc.

Appendix B

Measures of Likelihood and Impact/Severity

Diagram 1



Likelihood Measures

	Low	Medium	High
Probability	Less than 10% chance of circumstances arising	10% to 75% chance of circumstances arising	More than 75% chance of circumstances arising
Timescale	Is unlikely to occur	Possible in the next 1-3 years	Occurred in the past year or is very likely to occur in the next year

Impact / Severity Measures

	Low	Medium	High
People/Duty of Care	Low level of foreseeable minor injuries	Medium level of foreseeable minor injuries or low level of foreseeable serious injuries	High level of foreseeable severe long-term injuries or illness
Financial Impact	Up to £500k/Less than 5% over project budget	Up to £1 million/5 - 25% over project budget	Over £1 million/more than 25% over project budget
Legal Impact	Minor civil litigation	Major civil litigation and/or local/national public enquiry	Legal action by Section 151, Monitoring Officer, External Audit or government

Service Impact	Short term service disruption	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/council's performance
Intervention Required	Intervention by Service Manager, Project Manager or equivalent	Intervention by Head of Service or equivalent	Intervention by the Corporate Management Team, Board 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

Appendix C

Risk Response Categories

Categories	Description
Treat	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.
Tolerate	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 needs to be monitored.
Terminate	A decision is made to avoid 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.
Exploit	Whilst taking action to mitigate risks, a decision is made to exploit a resulting opportunity.

This page is intentionally left blank

Report of:	Meeting	Date	Item No.
Corporate Director Resources and s.151 Officer	Audit Committee	27 September 2022	

STATEMENT OF ACCOUNTS 2021/22, CAPITAL FINANCING AND REVENUE OUTTURN

1. Purpose of Report

1.1 To approve the council's published Statement of Accounts and the final capital and revenue position for the financial year 2021/22.

2. Outcomes

2.1 Evidence that the council produces accounts in accordance with relevant standards and timetables, supported by comprehensive working papers and promotes external accountability.

2.2 Compliance with the requirements of the Accounts and Audit Regulations.

3. Recommendations

3.1 The Chair is requested to:

i. Approve the Accounting Policies selected and applied by the Council, as required by International Accounting Standard No. 8: Accounting Policies, Changes in Accounting Estimates and Errors, which are set out as Note 2 to the Financial Statements attached;

ii. Approve the Council's Statement of Accounts 2021/22, subject to audit;

iii. Note the major variations in expenditure and income, the proposed slippage and the resulting impact on the level of the Council's reserves and balances at 31 March 2022; and

iv. Ensure that the accounts are subject to robust member scrutiny/discussion.

4. Background

4.1 The Accounts and Audit Regulations 2015 (as amended in March 2021) require the council's responsible financial officer to certify that the accounts 'present a true and fair view of the financial position' for the 2021/22 financial year by the 31 July 2022 (the date has been extended from 31 May as a result of the COVID-19 pandemic). This deadline has been achieved with the draft accounts being agreed by the S.151 Officer and published on the council's website on 29 July 2022.

4.2 The council is then formally required to approve and publish the Statement of Accounts no later than 30 September 2022 (the date has been extended from 31 July as a result of the COVID-19 pandemic). Following approval, the Statement of Accounts must be signed and dated by the member presiding at the meeting at which approval is given.

4.3 Owing to the well documented and reported audit delays across the sector, the council's 2020/21 Statement of Accounts are still awaiting formal sign-off. Achievement of post-audit sign-off for the 2021/22 accounts will be similarly delayed and both are expected to be signed off by 31 March 2023 or earlier, meaning that the regulatory deadline will not be met for a second year running. There are no financial penalties for exceeding the regulatory timescales but there can be a reputational impact. However, given the current context nationally and the issues beyond the control of the council and the wider sector, this is not considered to be a material concern.

4.4 Training materials for the statement of accounts for the 2021/22 financial year were circulated to the Chair and the rest of the Committee in June. This included a recorded training session for members to view online at their convenience.

5. Key Issues and Proposals

5.1 An Executive Summary setting out the main details in a format that is straightforward and easy to understand is included in the Statement of Accounts as part of the Narrative Report. The Narrative Report also includes non-financial information as part of the 'Telling the Story' requirement in the Code of Practice. The Statement of Accounts is attached at Appendix 1 for consideration, although this is still subject to audit.

5.2 The Capital Financing Report is attached at Appendix 2 (Table 1) and a comparison of actual capital expenditure to the 2021/22 updated revised budget, illustrating the nature of the variance e.g. advance spend, over spend, under spend or slippage to future years can be seen at Appendix 2 (Table 2).

5.3 A report identifying major variations in revenue expenditure and income compared to the levels budgeted for the year is attached at Appendix 3a and the proposed revenue slippage into 2022/23 and future years is

included at Appendix 3b.

5.4 The resulting impact of these changes, such as additional expenditure or reduced income, on the level of the Council's reserves and balances at 31 March 2022 is shown at Appendix 4.

IMPLICATIONS	
Finance	There are no immediate financial implications arising from this report. The final outturn position will be incorporated within the Medium Term Financial Plan 2022/23 to 2026/27 which aims to provide detailed proposals for corporately managing the council's resources in the years ahead and is subject to continuous monitoring to ensure its effectiveness.
Legal	The approval of the recommendation will help ensure that the statutory requirements have been complied with.

Other risks/implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

risks/implications	✓ / x
community safety	x
equality and diversity	x
sustainability	x
health and safety	x

risks/implications	✓ / x
asset management	x
climate change	x
ICT	x
data protection	x

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a third party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

Report Author	Telephone No.	Email	Date
Clare James	01253 887370	Clare.james@wyre.gov.uk	22.08.2022

List of Background Papers:		
Name of Document	Date	Where available for inspection
None		

LIST OF APPENDICES

Appendix 1 – Statement of Accounts for the year ended 31 March 2022
Appendix 2 (Table 1) - Capital Financing Report
Appendix 2 (Table 2) - Comparison of Capital Expenditure to Budget
Appendix 3a – Major Revenue Variances
Appendix 3b – Revenue Budget Savings - Slippage into Future Years
Appendix 4a – Reserves and Balances Statement
Appendix 4b – Transfers to and from Reserves

Document is Restricted

This page is intentionally left blank