Wyre Borough Council
Date of Publication: 7 November 2022
Please ask for : Daphne Courtenage
daphne.courtenage@wyre.gov.uk
Tel: 01253 887476

Audit Committee Agenda

Audit Committee meeting on Tuesday, 15 November 2022 at 6.00 pm in the Council Chamber - Civic Centre, Poulton-le-Fylde

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 27 September 2022.

4. **Internal Audit and Risk Management - Progress Report** (Pages 9 - 38)

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

5. **Annual Review of the Financial Regulations and Financial Procedure Rules** (Pages 39 - 42)

   Report of the Corporate Director Resources (Section 151 Officer), presented by the Head of Governance and Business Support.

6. **Annual Review of the Council's Counter Fraud Policies** (Pages 43 - 46)

   Report of the Corporate Director Resources (Section 151 Officer), presented by the Head of Governance and Business Support.

7. **Annual Review of the Council's Information Governance Policies and Procedures** (Pages 47 - 92)

   Report of and presented by the Head of Governance and Business Support (and Data Protection Officer).

8. Annual Review of the Audit Committee's Performance (Pages 93 - 102)

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

9. Appointment of the Council's External Auditors from 2023/24

Item for information. Update presented by the Corporate Director Resources (Section 151 Officer).

10. Statement of Accounts (pre-audit) 2021/22 (Pages 103 - 106)

Report of the Corporate Director Resources (Section 151 Officer). Deferred item from last meeting.

Please see attached link for appendices, included in the agenda for the last meeting
https://wyre.moderngov.co.uk/documents/b5514/Statement%20of%20Accounts%20pre-audit%20202122%20appendices%2027th-Sep-2022%2018.00%20Audit%20Committee.pdf?T=9.

11. Any other business

12. Date of next meeting

The next meeting of the Committee will be held on Tuesday 28 February 2023 at 6pm in the Council Chamber.

Audit Committee Minutes

The minutes of the Audit Committee meeting of Wyre Borough Council held on Tuesday, 27 September 2022 at the Committee Room 2 - Civic Centre.

Audit Committee members present:
Councillors McKay, Ingham, A Turner, Ibison, Longton, Moon and L Walmsley

Apologies for absence:
Councillors E Ellison, Leech, Minto, Stirzaker and Webster

Other councillors present:
None.

Failure to attend:
Councillors Fairbanks and George.

Officers present:
Clare James, Corporate Director Resources (and Section 151 Officer)
Joanne Billington, Head of Governance and Business Support
Karen McLellan, Audit and Risk Manager
Dawn Allen, Audit, Risk and Performance Lead
Mary Grimshaw, Legal Services Manager (and Monitoring Officer)
Stuart Kenny, External Auditor – Deloitte
Paul Hewitson, External Auditor – Deloitte
Daphne Courtenage, Assistant Democratic Services Officer

No members of the public or press attended the meeting.

---

12 Declarations of interest

None.

13 Confirmation of minutes

Councillor Moon asked a point of clarification on whether his apologies had been accepted for the previous meeting. The Assistant Democratic Services Officer assured him they had been included in the minutes.

The minutes of the last meeting of the Audit Committee held on 14 June 2022 were approved as a correct record.

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

The Legal Services Manager submitted a report to the committee to provide an update following a recent inspection on RIPA by the Investigatory Powers Commissioner's Office (IPCO) and to approve a revised RIPA policy.

She explained to the committee that there had been a virtual inspection in January 2022, and that a summary of the inspection had been included the report. The inspector had been satisfied that the council had demonstrated a level of compliance that negated the need for an onsite inspection, was satisfied with the council's policy, training of officers and the guidance given for the use of the internet and social media.

The inspector did however recommend amendments to the communications data section to reflect recent legislative changes. These changes included the ability to obtain details of in and out call data and cell site location. All changes to the policy could be seen in the track changes in Appendix 1 of item 4 of the agenda pack.

The Legal Services Manager told the committee that the council had not made any RIPA applications since 2012, which was very good, but still needed to comply with the legislation and the inspection regime.

It was agreed that the update was noted and the revised RIPA policy approved.

15 Annual Review of the Council's Risk Management Policy

The Corporate Director Resources (S151 Officer) submitted a report to the committee 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.

The Audit, Risk and Performance Lead introduced the report. She explained to the committee that this was an annual review, and that there were very little changes from last year. These changes were in relation to the frequency of review and risk action email notifications; the risk review notifications would now go out quarterly and the risk action notifications would go out two weeks prior to the due date of the action plan.

Councillor Moon asked about the use of the risk register. The Audit, Risk and Performance Lead responded that once a risk was in the register, it would be given a score and an action plan generated. Any risks that were closed would be reviewed by Internal Audit, so all registered risks would be thoroughly reviewed.

Councillor Ibison asked about how risks were categorised numerically, and whether urgent risks had a particular timescale. The Audit, Risk and Performance Lead explained that the actions put against the risks would

include timescales and the action plan due dates would prompt a notification to review, update or close the risk. Every quarter, the system would be reviewed.

The report was noted and it was agreed that the refreshed Risk Management policy was approved.

16 Statement of Accounts (pre-audit) 2021/22

The Corporate Director Resources (S151 Officer) submitted a report to the committee to approve the council's published Statement of Accounts and the final capital and revenue position for the financial year 2021/22.

The Corporate Director Resources attended the meeting virtually, gave apologies on behalf of the Head of Finance, and explained that they were both adhering to Covid-19 isolation guidance owing to symptoms. Rather than go through the detailed question and answer session on the Statement of Accounts at this meeting, she proposed that she would circulate the document to the committee the following week, so they could review this, with additional comments from herself on points she believed needed to be brought to the committee's attention. This would give the committee the opportunity to thoroughly review the document and the Statement of Accounts, and at the next proposed meeting on November 15 2022, there would be a quick overview and the formal sign-off of the draft Statement of Accounts.

She assured members that there was no great urgency in getting the draft signed off, as the audit had not yet started, and they could afford to defer the vote to the next meeting.

Councillor Moon asked the Chair about ensuring that there was sufficient scrutiny and questioning of the Statement of Accounts. The Chair responded that she thought having the time in-between this meeting and the next meeting would be more useful, as well as the question and answer document supplied by the Corporate Director, rather than going through it all in one meeting.

The Chair asked a question to the Corporate Director and the external auditor from Deloitte on updates on the timing of the audit.

The Corporate Director said she knew meetings were ongoing, but that the issue on the infrastructure assets which had been mentioned in the meeting of the 14 June 2022 had still not been resolved by CIPFA.

Stuart Kenny, the external auditor from Deloitte, told the committee that the 2020/21 accounts were still waiting to be signed off owing to the infrastructure assets issue. They were waiting for the Department for Levelling Up to issue a draft statutory instrument to resolve these issues, though it was still to be seen whether this would completely resolve the issue. In terms of 2021/22, the infrastructure assets would still have an impact on this, and would likely

mean changes to the draft statement of accounts, but at the moment these changes were not clear. In terms of the actual audit, they were still discussing the timescale for it.

The Chair asked a follow up question as to whether the deadline for the 2020/21 accounts would still be March 2023.
Mr Kenny responded that if the infrastructure asset issue could be resolved in time, then the deadline would remain for both sets of accounts as March 2023.

The committee agreed to defer the discussion and agreement on the draft Statement of Accounts to the next meeting.

17 Exclusion of the public and press

In accordance with Paragraph 11 of the Access to Information Rules in Part 4 of the Council's Constitution, the Chief Executive had determined that the report submitted under item 8 of the agenda were "Not for Publication" because they contained "exempt information", as defined in Schedule 12A of the Local Government Act 1972.

The Committee passed the following resolution: "That the public and press be excluded from the meeting whilst agenda item 8 was being considered, as it referred to exempt information as defined in category 3 (information relating to the financial or business affairs of any particular person including the authority holding that information) and category 5 (information in respect of which a claim to legal professional privilege could be maintained in legal proceedings) 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 exemption outweighed the public interest in disclosing the information.

18 Draft Annual Governance Statement 2021/22 update

The Corporate Director Resources (S151 Officer), alongside the Head of Governance and Business Support and the Audit and Risk Manager, gave a verbal update to the group on amendments required for the draft Annual Governance Statement, which had been presented to the committee at the last meeting.

The Corporate Director explained to the committee the reasons for the amendments, as well as the situation which preceded these amendments.

The committee asked questions of the Corporate Director, the Head of Governance and Business Support and the Audit and Risk Manager, on the situation which had also been presented in the report to Cabinet in September, which had been included as part of this agenda.

The committee agreed to the amended wording proposed by the Corporate Director Resources and would agree the final Annual Governance Statement

as part of the deferred Statement of Accounts item in November.

19 Periodic private discussion with External Audit

Following the conclusion of the formal meeting, members of the committee were given the opportunity to have their private periodic discussion with the external auditors, Stuart Kenny and Paul Hewitson, as provided for in the committee's work programme.

(The Corporate Director Resources (S151 Officer), the Head of Governance and Business Support, the Audit and Risk Manager, the Audit, Risk and Performance Lead, and the Assistant Democratic Services Officer, left the meeting for this item).

The meeting started at 6.00 pm and finished at 6.50 pm.

Date of Publication: 28 September 2022

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	15 November 2022

INTERNAL AUDIT AND RISK MANAGEMENT PROGRESS REPORT

1. Purpose of report

1.1 To review progress in relation to the 2022/23 audit plan and risk management and to consider progress against the action plan resulting from the 2021/22 Annual Governance Statement (AGS).

2. Outcomes

2.1 Effective leadership of audit and governance issues allowing the council to demonstrate that arrangements are in place to maintain a sound system of internal control.

3. Recommendation

3.1 Members are asked to note the progress reports attached at Appendices 1, 2 and 3.

4. Background

4.1 The Audit Committee has a clear role in relation to the authority's internal audit function and this involves:

- Formally approving, but not directing, the overall strategy to ensure that it meets the council's overall strategic direction;
- Approving the annual programme of audits paying particular attention to whether there is sufficient and appropriate coverage and;
- Monitoring progress against the plan and assessing whether adequate skills and resources are available to provide an effective audit function.

4.2 The Audit Committee's role in relation to reviewing the work carried out will include formal consideration of summaries of work done, key findings, issues of concern and actions planned as a result of audit work. A key part of the role is receiving and reviewing regular reports from the Audit

and Risk Manager (Chief Internal Auditor) in order to reach an overall opinion on the internal control environment and the quality of internal audit coverage.

5. Key Issues and proposals

5.1 The progress reports in relation to Internal Audit, Risk Management and the action plan resulting from the 2021/22 AGS are attached at Appendices 1, 2 and 3.

Financial and legal implications	
Finance	There are no financial implications that impact the Internal Audit and Risk Management progress report. The in-house team performs the annual programme of audits.
Legal	Effective audit and 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 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 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
Karen McLellan	01253 887586	Karen.mclellan@wyre.gov.uk	4 November 2022

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

List of appendices

Appendix 1 – Internal Audit Progress Report

Appendix 2 – Risk Management Progress Report

Appendix 3 – Annual Governance Statement 2021/22 - action plan update

Appendix 1

INTERNAL AUDIT PROGRESS REPORT – APRIL to NOVEMBER 2022

THE AUDIT PLAN AND DELIVERY

The Internal Audit and Risk Management Section is responsible to the Corporate Director Resources (Section 151 Officer) for carrying out a continuous examination of the accounting, financial and other operations of the council in accordance with Section 151 of the Local Government Act 1972 and the Accounts and Audit Regulations 2015 (as amended in 2021). The latter states that ***"the relevant body shall be responsible for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of that body's functions and which includes arrangements for the management of risk."***

The table overleaf summarises audit work performed since the last progress reported at the Audit Committee meeting on 14 June 2022. Copies of both terms of reference and internal audit reports are published on the council's hub and the councillor's portal and access to the supporting files are available on request.

Wyre Council attends the Lancashire District Council's Audit Group and continues to participate in the Cabinet Office National Fraud Initiative data sharing exercise. The Insurance and Business Continuity Officer now participates in the North West Insurance Officer Group with other local authorities across Lancashire.

Internal Audit will continue to provide the council with the necessary assurance about its various activities and associated systems, as outlined in the council's Internal Audit Charter which is reviewed and approved by the Audit Committee annually.

All audit work that forms the annual audit opinion is completed by the in-house team. However, the ICT support framework managed by Lancashire County Council is still available should additional expertise be required in this specialised area.

Internal audit work is benchmarked where possible with other local district councils who participate in the Public Sector Internal Audit Standards (PSIAS) peer reviews to ensure that quality and standards are maintained. In addition, the standardised working papers along with a robust review process prior to report publication, ensures continual conformance to the PSIAS, consistency and high standards of reporting are maintained.

An electronic feedback questionnaire has been introduced during 2022/23 to obtain feedback on all completed audit reviews. A summary of this feedback will be provided to the Audit Committee in June 2023 as part of the annual opinion.

Audit Work Performed April to November 2022

Mid-way through 2021/22 a decision was taken to change the previously used audit opinions to be in line with other local authorities. Therefore some of the audit opinions (follow-up work from 2021/22) in the table below reflect the previous definitions. The priority rankings for audit actions remain the same. As summarised below the following reviews have been performed and reports issued since the annual audit reported in June 2022.

AUDIT OPINION DEFINITIONS (April – November 2021)

Excellent	Controls are in place to ensure the achievement of service objectives, good corporate governance and to protect the Council / Partnership against significant foreseeable risks. Compliance with the risk management process is considered to be good and no significant or material errors or omissions were found.
Good	Controls exist to enable the achievement of service objectives, good corporate governance and reduce significant foreseeable risks. However, occasionally instances of failure to comply with the control process were identified and opportunities still exist to reduce potential risks.
Fair	Controls are in place and to varying degrees are complied with but there are gaps in the control process, which weaken the system and leave the Council / Partnership exposed to some minor risk. There is therefore the need to introduce some additional controls and improve compliance with existing controls to reduce the risk to the Council / Partnership.
Weak	Controls are considered inefficient with the absence of at least one critical control mechanism. There is also a need to improve compliance with existing controls, and errors and omissions have been detected. Failure to improve controls leaves the Council / Partnership open to significant risk, which could lead to major financial loss, embarrassment or failure to deliver service objectives.
Poor	Controls are generally weak or non-existent leaving the system open to abuse or error. A high number of key risks remain unidentified and therefore unmanaged.

AUDIT OPINION DEFINITIONS (November 2021- November 2022)

Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
Minimal / No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
Inspection Regime – Site Inspections (follow up)	**Fieldwork in progress**							The overall objective of the audit is to follow up the findings originally reported in the 2019/20 audit review and which were found to be outstanding in 2021/22 and to identify any further areas of potential weakness and / or risk and provide an overall opinion on whether the controls in place are managed adequately and effectively.
Beach Management Scheme	**On-going**							The Audit and Risk Manager continues to attend the monthly beach management project meetings to provide advice and support in respect of internal control, risk management and governance procedures. It is not anticipated that a report will be published in relation to this work. However, an overall opinion on the control environment in relation to this project will be provided in the Internal Audit Annual report for 2022/23.
Project Neptune	**Project complete**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Reasonable Assurance**	Project Neptune was successfully completed on the 10 August 2022 resulting in the ownership of the constructed buildings being formally passed to the council. Responsibility for the ongoing implementation and management of the tenancy arrangements and agreements has been passed to the Estates Team. Whilst an overall report has not been produced for this project, for the purpose of this report an overall opinion of 'reasonable' is appropriate.
Covid-19 grants Post assurance testing	**Completed No final report issued**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Substantial Assurance**	Following the introduction of the Covid-19 business grants in April 2020, pre and post assurance work required by the Department for Business, Energy and Industrial Strategy (BEIS) has continued during 2022. All councils were requested to submit supporting evidence in respect of all the business grants received during 2020/21.

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								Whilst an overall report has not been produced for this post assurance work, for the purpose of this report an overall opinion of 'substantial' is appropriate. Working papers are in place to support this opinion. Should the compliance certificate be returned by BEIS as a fail, this area and opinion will be revisited.
Matrix Agency Staff contract (follow up)	**Final report issued October 2022**	**0**	**0**	**0**	**0**	**0**	**Reasonable**	The original review of the Matrix Agency contract was completed in January 2022 as part of the 2021/22 audit plan and given an overall opinion of 'Limited'. A follow up has been completed as part of the 2022/23 audit plan and of the 5 findings originally reported all of these have now been implemented. Whilst all the original recommendations have been implemented, the overall opinion has been graded as 'reasonable' due to the high possibility that services will still continue to procure agency staff without consulting HR. A further action has been added to try and mitigate this risk and this will be monitored through the GRACE risk management system.
Citizen Access Portal and council website	**Draft report Issued**							The overall objective of the audit is to review the controls in place around the management and ongoing development of the Citizens Access Portal and council website and to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.
Data Protection Policy and process review	**Draft report issued**							The overall objective of the audit is to review the controls in place around the management of the Data Protection Policy and UK General Data Protection Regulations to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
Market House Studios	**Final report issued June 2022**	**0**	**2**	**4**	**0**	**0**	**Reasonable**	Areas have been identified where improvements could be made to strengthen the control environment, namely: • A review of the service objectives established prior to the Covid-19 pandemic now need reviewing and adapting to reflect current operations; • A procedural manual covering all aspects of the day to day operation of the studios is required; • The completion of an annual appraisal for the Studio Co-ordinator is required documenting personal objectives / targets; • All cash income received must be banked promptly; • Staff training on the Civica system is required to assist the monitoring of rent arrears and budget monitoring; • All completed risk assessments must be agreed and signed off with tenants; As this review has received a reasonable assurance opinion, a further follow-up is not required. However, the implementation of the recommendations will be monitored through the GRACE risk management system.
Fleetwood and Poulton Markets	**Final report issued August 2022**	**0**	**10**	**2**	**0**	**0**	**Reasonable**	Areas have been identified where improvements could be made to strengthen the control environment, namely: • A service plan for the Fleetwood and Poulton Markets has yet to be finalised; • The recording of TOIL balances and annual leave allowances are not always accurately recorded on the CROWN time recording system;

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								• Staff appraisals have not been completed during 2021 and must be completed by the end of January 2023; • Further training on the operation of the CCTV system at the market is required together with the completion of spot checks of all viewings of recorded data; • The information asset register compiled by the Estates Team or CCTV Service requires updating to include the Market CCTV system; • Evidence of all current public liability insurance policies held by permanent and casual tenants occupying market stalls is required; • Evidence of the contractual agreement for the cash machine located at the market is required to review terms and conditions; • The issue of a purchase card replacing the petty cash float should be considered to avoid delays in the reimbursement of this float; • The monthly management meetings during which rent arrears are discussed should be re-introduced; • Two actions identified during the 2021 health and safety building audit relating to the electrical remedial works and the completion of actions arising from the 2021 legionnaires risk assessment have yet to be fully implemented; • Site security during non-trading days must be maintained whilst contractors are on site to prevent unauthorised access; and • Three actions arising from the 2021 review of cash handling still require implementing i.e. cash office risk assessment / installation of a card payment facility and replacement

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								cash till. As this review has received a reasonable assurance opinion a further follow-up is not required, however, the implementation of the recommendations will be monitored through the GRACE risk management system.
Business Health Matters Programme	**Fieldwork in Progress**							The overall objective of the audit is to review the controls in place around the management of the business health matters programme and to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.
Building Maintenance Re-active Repairs framework	**Fieldwork in Progress**							The overall objective of the audit is to review the controls in place around the management of the building maintenance re-active repairs framework to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.
Elections Accounts (post assurance)	**Fieldwork in progress**							The overall objective of the audit is to review the controls in place around the completion of the 2021 election accounts to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.
Main Accounting - Key Financial Risk Matrix (KFRM)	**Fieldwork in progress**							The overall objective of the completion of a key financial risk matrix is to review the controls in place around the main accounting systems and processes to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
Treasury Management - Key Financial Risk Matrix (KFRM)	**KFRM issued to Head of Service (Finance)**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Substantial**	Following the turnover of staff in the Finance Team during 2020-22 resulting in a number of vacant posts and a loss of knowledge / experience within the team, a key financial system matrix has been completed to document all controls in relation to the Treasury Management system / process to identify any areas requiring improvement. Only one area was identified that required strengthening in relation to the documented staff procedures, which require updating. Whilst a formal report has not been published in relation to this work, for the purpose of this report 'substantial assurance' has been given. Working papers are in place to support this opinion. No follow-up review is required, however, the implementation of the recommendation made will be monitored using the GRACE risk management system.
Budgetary control - Key Financial Risk Matrix (KFRM)	**KFRM issued to Head of Service (Finance)**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Reasonable**	Following the turnover of staff in the Finance Team during 2020-22 resulting in a number of vacant posts and a loss of knowledge / experience within the team, a key financial system matrix has been completed to document all controls in relation to the Budgetary control system / process to identify any areas requiring improvement. The following observations was made which require strengthening in relation to the following: • The guidance / procedure notes covering the tasks to be completed require updating; • Access permissions to the Civica system require reviewing for all council leavers; • The completion of quarterly budget meetings with budget holders has been delayed due to ongoing staffing issues; • Monthly budget reports are issued to budget holders, but confirmation of their review of

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								these reports is not requested. Whilst a formal report has not been published in relation to this work, for the purpose of this report 'reasonable assurance' has been given. Working papers are in place to support this opinion. No follow-up review is required, however, the implementation of the recommendations made will be monitored using the GRACE risk management system.
Creditors - Key Financial Risk Matrix (KFRM)	**KFRM issued to Head of Service (Finance)**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Reasonable**	Following the turnover of staff in the Finance Team during 2020-22 resulting in a number of vacant posts and a loss of knowledge / experience within the team, a key financial system matrix has been completed to document all controls in relation to the Creditors system / process to identify any areas requiring improvement. Two observations was made which require strengthening in relation to the following: • Staff resourcing issues across the service still exist; • Civica system reports identifying the retrospective issue of purchase orders are issued but no action is currently taken to address non-conformance to policy / procedure. Whilst a formal report has not been published in relation to this work, for the purpose of this report 'reasonable assurance' has been given. Working papers are in place to support this opinion. No follow-up review is required, however, the implementation of the recommendations made will be monitored using the GRACE risk management system.
Expenses - Key Financial Risk Matrix	**KFRM issued to Head of**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Reasonable**	Following the turnover of staff in the Finance Team during 2020-22 resulting in a number of vacant

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
(KFRM)	**Service (Finance)**							posts and a loss of knowledge / experience within the team, a key financial system matrix has been completed to document all controls in relation to the Expenses system / process to identify any areas requiring improvement. The following observations were made which require strengthening in relation to the following: • A number of procedural documents require updating or removing from the Hub; • The procedure for processing the expenses interface should be documented and made available to all staff; • Training should be provided to another officer to complete the expenses interface during the absence of the Financial Systems and Reporting officer. Whilst a formal report has not been published in relation to this work, for the purpose of this report 'reasonable assurance' has been given. Working papers are in place to support this opinion. No follow-up review is required, however, the implementation of the recommendations made will be monitored using the GRACE risk management system.
Payroll - Key Financial Risk Matrix (KFRM)	**KFRM issued to Head of Service (Finance)**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Limited**	Following the transfer of Payroll from HR to Finance in July 2021, a key financial system matrix has been completed to document all controls in relation to the Payroll system / process to identify any areas requiring improvement. The following observations were made which require strengthening; • The current staffing structure does not allow for an appropriate segregation of duties to be maintained within the payroll process; • The Financial Systems and Reporting

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								Officer (FSRO) is the only officer within the Financial Services team with the required knowledge to complete the payroll processes; • The payroll procedures / process is not documented to assist officers when completing the payroll processes during the absence of the FSRO. Whilst a formal report has not been published in relation to this work, for the purpose of this report 'limited assurance' has been given. Working papers are in place to support this opinion. A further follow-up is therefore scheduled to be carried out in January 2023 to ensure the observations made have been addressed.
VAT - Key Financial Risk Matrix (KFRM)	**KFRM issued to Head of Service**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Reasonable**	Following the turnover of staff in the Finance Team during 2020-22 resulting in a number of vacant posts and a loss of knowledge / experience within the team, a key financial system matrix has been completed to document all controls in relation to the VAT system / process to identify any areas requiring improvement. The following observations were made which require strengthening; • Finance staff are not always informed of large projects that have VAT implications impacting the partial exemption limit; • Compliance checks are not routinely completed to ensure VAT is being accurately recorded by staff when processing or raising invoices; Whilst a formal report has not been published in relation to this work, for the purpose of this report 'reasonable assurance' has been given. Working papers are in place to support this opinion. No follow-up review is required, however, the

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								implementation of the recommendations made will be monitored using the GRACE risk management system.
Procurement including The Chest portal - Key Financial Risk Matrix (KFRM)	**Fieldwork in progress**							The overall objective of the completion of a key financial risk matrix is to review the controls in place around the Procurement systems and processes to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.
Debtors and Recovery - Key Financial Risk Matrix (KFRM)	**Fieldwork in progress**							The overall objective of the completion of a key financial risk matrix is to review the controls in place around the Debtors and Recovery systems and processes to identify any areas of potential weakness and / or risk and provide an overall opinion as to whether the controls in place are managed adequately and effectively.

Outstanding work to be completed in 2022/23 (ending 31 March 2023)

- National Fraud Initiative (NFI) – Annual NFI exercise (Inc. Single Person Discount Data Matching exercise)
- Civica Pay
- Marine Hall/Thornton Little Theatre/Mount Pavilion - continual review
- Grant schemes – compliance with terms and conditions
- Performance management – development of the new process
- Assurance mapping to assist the compilation of the 2023/24 audit plan
- On-going preparation for the internal audit PSIAS peer review in March 2023

Other audit work undertaken during the year 2022/23

National Fraud Initiative – Cabinet Office data matching exercise

Since the last NFI update presented to the Audit Committee in June 2022, some progress has been made to investigate the matches resulting from the 2020/21 council tax single person discount data matching exercise. Whilst the Compliance Team have been unable to investigate any of these data matches due to competing work pressures and their involvement in processing the remaining Covid-19 business grant payments and energy rebates, training was provided to the Corporate Apprentices and the Insurance and Business Continuity Officer to assist with the investigation of the matches produced. However, whilst a large number of matches have been investigated by these officers, due to the age of the data, the issue of letters to residents requesting additional information has been delayed pending receipt of the next data exercise in January 2023. The revised data will then be reviewed and compared to the matches already investigated and the system updated. A further progress update will be provided to the Audit Committee in June 2022.

Information Governance - Compliance with the Data Protection Act 2018 and UK GDPR

The council's Data Protection Officer (DPO) supported by the Information Governance Group (IGG) continue to work together to ensure the council is compliant with data protection legislation. The DPO, Deputy DPO and the Audit and Risk Manager continue to support officers across the council in ensuring the council's data protection obligations are met and the DPO reports quarterly to the Corporate Management Team (which includes the SIRO), with the last update being on 14 September 2022 and the next update being scheduled for 1 February 2023. The following areas were reported at the last update;

- The scope in relation to the Data Protection and UK GDPR compliance audit was recently widened to include a more detailed examination of the council's information asset registers. Whilst information asset registers are in place for the majority of the main services, these registers are mostly out of data and have not been reviewed for some time. There are also some services that don't have any records of the information they hold. In lights of this, the auditor feels a more true reflection of the assurance level is 'limited assurance' to reflect the significant gaps with the information asset registers. A report has now been drafted and the actions have been agreed with the IGG. Information Asset Registers and the importance of these will be discussed at the Head of Service meeting on 9

January 2023, following which an exercise will begin to ensure all services have information asset register in place.

- The Subject Access Request Procedure has now been finalised and approved by CMT. The Audit Committee will receive the procedure in November for final approval along with the refreshed Records Management Policy and updated Data Protection Policy and Procedure.

- Learning Pool – The cyber security module has now been rolled out to all staff. Completion rates are being monitored by HR and ICT and regular reminders will continue to be sent out until all staff have completed the mandatory module. Once all staff have completed this, the data protection module will then be rolled-out. It has been agreed with HR and ICT that both of these modules will be completed by new starters on their first day.

- Cyber / Disaster Recovery – key risks continue to be monitored through the GRACE risk management system and are reviewed on a quarterly basis by the Corporate Director Resources, Head of Service, Audit and Risk Manager and the ICT Service Delivery Lead. The council continue to work on a number of solutions for cyber / disaster recovery, which to date has included identifying more back-up sites, completing a Cyber Resilience Self-Assessment (currently 2/3 completed) to identify the gaps and the key risks and drafting both a Cyber Resilience and Disaster Recovery Plan. Due to limited resources, progress is slow, however it is hoped that both plans will be finalised in 2022.

- The DPO continues to log and investigate all data incidents. Since April 2022, two data incidents have been reported to the ICO, one of which has resulted in the council receiving a letter from a solicitor. A response has been issued by the DPO and the council is currently awaiting a response.

- The IGG have recently refreshed the council's ICT Computer Use Policy and User Agreement. This was approved by Full Council on the 27 October 2022. It will now be rolled out to all staff and Elected Members, who will need to complete the mandatory declaration confirming their understanding and compliance to the Policy.

<u>Anti-Fraud and Corruption</u>

All the council's counter fraud policies are reviewed annually by the Audit Committee, with the last review being completed in November 2022. The policies are located on the Hub to allow staff and Elected Members easy access. The council's four counter fraud policies are as follows;

- Counter Fraud, Corruption and Bribery;
- Anti-Money Laundering;
- Gifts, Hospitality and Registering Interests, and;
- Whistleblowing.

Anti-Money Laundering - To date, there has been no reports of suspected money laundering during 2022/23.

Gifts, Hospitality and Registering Interests – There have been no declarations made by council officers receiving gifts and hospitality since the 21 January 2022. A reminder

will go out in the December Core Brief for staff to use the on-line form to register any gifts or hospitalitlity received and to report any registered interests they may have in relation to council business.

Whistleblowing / Investigations - There has been one internal investigation and one whistleblowing call since 1 April 2022.

The investigation which has now concluded, was reported to the Audit Committee in September 2022. As advised at that meeting, following a disciplinary hearing held by the Corporate Director Environment an outcome of gross misconduct was reported and as a result, the officer was dismissed.

A whistleblowing call was received on 18 August 2022. This is currently in the process of being investigated by the Audit and Risk Manager and the Head of Governance and Business Support. The Audit Committee Chairman has been provided with an overview of the whistleblowing and a further update will be provided to the Audit Committee once the investigation has been completed.

RISK MANAGEMENT PROGRESS REPORT

Progress on the embedding of risk management is reported to the Audit Committee via six monthly reports by the Audit and Risk Manager. This is in line with the council's Risk Management Policy, originally approved by Cabinet in April 2004 and reviewed and approved annually by the Audit Committee.

The council's strategic, operational and ICT risks are now populated within the risk management system (GRACE) and action plans have been added to assist with the mitigation of the risks identified.

Strategic Risks

The Corporate Management Team (CMT) met on 18 March 2022 to carry out the annual strategic risk workshop. The results of the workshop were presented to the Audit Committee at its meeting in June 2022. At the workshop, significant business risks that may impact upon the council's priorities (the business plan) were identified and assessed, and appropriate control measures were put place. Progress is monitored on a quarterly basis by CMT, including a more comprehensive six monthly review which was completed on 12 October 2022. The results of this review will be reported verbally to the Audit Committee on 15 November 2022.

The next strategic risk workshop will be held on the 12 January 2023.

Operational Risks

Operational risk workshops were held this year following the strategic risk workshop in March, with each service unit identifying new risks that could occur during the year preventing the achievement of individual service plans. Whilst staff who have responsibilities for identified risks are encouraged to review their risks and update their action plans continually throughout the year, prompts have been issued to staff during the year to ensure progress was being documented. Individual operational risk registers have not been provided as part of this report as operational risks are reported to the Audit Committee on an 'exceptions' basis where any risks are not managed appropriately.

The Audit Committee are encouraged to go and view the risks identified by each service unit on the Councillor Portal (link below) and challenge any areas were limited progress is being made to mitigate the risks identified.

https://wyregovuk.sharepoint.com/sites/Councillor-Portal

ICT Risks

The council's ICT risk register is reviewed quarterly by the Corporate Director Resources, Head of Contact Centre and Interim Head of ICT, ICT Services Manager, Audit and Risk Manager and the Audit, Risk and Performance Lead. The last review was completed on 3 August 2022 and the updated register is available on the Hub.

ANNUAL GOVERNANCE STATEMENT 2021/22 - ACTION PLAN UPDATE

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
ICT Disaster Recovery / Cyber Resilience	C/F 2018/19	Whilst an ICT disaster recovery plan was initially drafted in 2018/19 this has yet to be finalised. Whilst some work has been completed to ensure the council is protected as much as possible from cyber-attacks, including carrying out a self-assessment of gaps/key risks, the council has still to progress a separate Cyber Resilience Plan.	The Disaster Recovery Plan needs to be finalised and rolled out as soon as possible. A separate Cyber Resilience Plan needs to be developed to take into consideration the issues raised in the recent cyber self-assessment.	Lee Brophy/ Peter Mason TBC Peter Mason/ Steph Wright 31 December 2022	The Disaster Recovery Plan still needs to be finalised and rolled out. The Cyber Resilience Plan still needs to be developed to take into consideration any issues raised in the cyber self-assessment currently being completed.
Climate Change	2021/22	The council declared a climate emergency in July 2019 and since this time the council has been working through a comprehensive action plan of issues effecting both council services and the wider community. Whilst good progress has been made in implementing a number of these actions, for example securing £1.2m in grant funding for the decarbonisation of Fleetwood Market and accredited as a Bronze level Carbon Literate Organisation, there is currently only one full time officer leading on climate change. Further work is needed to identify any gaps with the action plan and highlight the key projects (e.g. developing a	More staff need to be encouraged to take part in the Carbon Literacy training to facilitate the achievement of a silver accreditation. In addition, lead officers need to be identified to drive forward the key projects to allow progression of the action plan which will allow the council to reduce its carbon emissions by at least 78% by 2035, in line with the UK government targets.	Mark Billington / Kathy Winstanley Sammy Gray	Key officers have been identified to lead on key projects with updates reported quarterly to CMT and management board.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
		strategy) and then nominate lead officers.			
Social Value	2021/22	Whilst the Council's Constitution considers social value when procuring goods and services and gives some advice, the council does not record or monitor the impacts / outcomes of social value following the procurement of goods and services. Initial investigations were made to procure software that would assist with the recording and monitoring of social value, however it was considered excessive for the council's current needs.	More work needs to be completed in regard to monitoring the impacts / outcomes of social value, particularly with larger contracts, following the procurement of goods and services. Legislation is awaited which will influence any changes.	Lee Rossall	The new Public Procurement Bill has not yet been passed and in the meantime the council is working within the guidelines of the Public Services (Social Value) Act 2012. Further consideration will be given to including social value weightings in tender documentation and identifying other measures for monitoring social value outputs in contracts e.g. KPI's
Internal Audit Quality Assurance Improvement Programme (QAIP)	2021/22	From 1 June 2021 the Chief Internal Auditor role was allocated to the Audit and Risk Manager. However whilst the postholder has significant audit experience and has already obtained 'Certified' auditor status, she currently does not hold 'Chartered' status as required by the Public Sector Internal Audit Standards. Succession plans are in place within the	Whilst the Audit, Risk and Performance Lead obtains the necessary 'Chartered' status, the Head of Governance and Business Support will need to countersign the Internal Audit Self Effectiveness review and also the Annual Audit	Jo Billington / K McLellan	Completed

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
		Internal Audit Team and given the current Chief Internal Auditor has indicated she may wish to retire in 2023/24, a decision has been made to allow the Audit, Risk and Performance Lead to undertake the relevant 'Chartered' qualifications.	Opinion. The QAIP needs to be updated to reflect this countersignature arrangement and the requirement for the Audit, Risk and Performance Lead to undertake the necessary 'Chartered' status.		
Report Author Training	2021/22	Whilst a number of changes have been made to the Constitution over the last few years, it is noted that the Report Author Guidance has not been refreshed since 2017, when the last training session for report authors was delivered. It is understood that the introduction of a 'climate change decision wheel' is to be introduced to the decision making process which will also need reflecting in the guidance.	The Report Author Guidance needs to be updated to include any changes made since 2017. It should also include guidance on the new 'climate change decision wheel'. Following which training will need to be arranged with all report authors.	Democratic Services	Report Author training has now been completed with a mop-up session scheduled for early November. The climate change decision wheel is currently being piloted with all key council decisions.
Regulation of Investigatory Powers Act (RIPA)	2021/22	Following the last inspection in January 2022, a few minor changes are needed to the council's RIPA Policy.	The RIPA policy needs to be reviewed and amended to take into consideration the minor changes recommended by the Inspector in January 2022.	Mary Grimshaw	Completed

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
Whistleblowing	2021/22	Following a recent whistleblowing and an external independent assessment of the council's policy and procedures, it was identified that the current policy needs reviewing.	A review of the WB Policy needs to be completed and submitted to the Audit Committee in November 2022 for approval. Following this, the policy will then need to be rolled out to all staff, partners and contractors.	Jo Billington	The Whistleblowing Policy has been reviewed and will be submitted to Audit Committee for approval on the 15 November 2022. Once approved it will be rolled out to staff, partners and contractors.
Information Governance / Data Protection (inc. Transparency Code)	C/F 2018/19	The council continues to work towards ensuring full compliance with the UK GDPR. Whilst the GDPR compliance audit included in the 2021/22 audit plan has yet to be finalised, 'reasonable' assurances have been given by the Auditor that generally there are sound controls in place and that whilst some areas have been identified that require strengthening, the auditor is confident that the majority of the issues identified can be addressed relatively quickly. However, a larger piece of work is needed by service managers to bring the information assets registers up to date. Elected Members have not had any data protection training since 2018. Whilst there will be a module within Learning Pool, there is no plans at this stage to roll out	The draft report for the GDPR compliance audit, which includes recommendations relating to compliance to the Transparency Code needs to be issued asap. The action plan needs to be managed by the Information Governance Group and regular updates need to be provided to CMT through the quarterly Head of Governance and Business Support updates. Need to arrange UK GDPR refresher training for the newly Elected Members in May 2023.	Jo Billington / Jo Porter / Dawn Allen / Karen McLellan Jo Billington / Democratic Services May 2023	The GDPR audit has now been completed and the action plan was considered by the Information Governance Group on the 5 October 2022. Once finalised, the implementation of the actions will be monitored through GRACE and CMT quarterly updates. GDPR refresher training has been arranged for the newly Elected

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
		the platform to Elected Members. However an alternative will be sourced.			Members on the 6 July 2023.
Staff Survey	C/F 2019/20	Whilst a full staff survey has not been carried out since 2017/18, there have been a number of staff engagement activities that have taken place; hybrid working and listening sessions at Marine Hall. However, these sessions may not have captured all staff giving every officer an opportunity to raise or voice concerns.	Consideration should be given to carrying out a full staff survey following the pandemic and the introduction of hybrid working, focusing on health and wellbeing following a difficult two years.	Jane Collier / CMT	A staff survey was carried out December 2020 – January 2021. The employee survey took a different approach to previous formats recognising the impact pandemic has had on staff. The survey gave the opportunity for staff to share the extent to which they are managing with new working arrangements and the impact the months since the start of the first lockdown in March 2020 have had on their wellbeing. In addition it was important to ascertain what staff think went well, not so well and what could have been done differently. The results from the

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
					survey have helped to form the basis for work carried out on the roll out of hybrid working from September 2021.
Corporate Comments, Compliments and Complaints Procedure	C/F 2019/20	The staff ethical governance survey carried out in October 2018 identified that although staff were aware that the council had a corporate Comments, Compliments and Complaints Procedure, they were less familiar with the content and where to locate it. In addition, it has become apparent that there are limited number of senior officers available to carry out second stage investigations. In response to these findings, the Corporate Apprentices surveyed CMT / HOS to try and capture any issues with the current processes with the object of refreshing the policy and identifying more resources to assist with second stage investigations. Whilst a summary of findings was produced, these have yet to be actioned.	The work completed by the Corporate Apprentices regarding the operation of the corporate Comments, Compliments and Complaints Procedure needs to be finalised with consideration be given to identifying additional resources for the second stage investigations.	Peter Mason / Jo Billington CMT / Jane Collier December 2022	Corporate complaints are now administered through the CXM system which has simplified the process. However, resources for completing second stage reviews are still stretched. HR are in the process of identifying future 'aspiring leaders'. Following this, consideration should be given to including them in the allocation of second stage reviews.
Competencies, behaviours and values	2021/22	The council's current values framework, which includes the expected values and behaviours, has not been reviewed following the role out of the hybrid working	HR need to continue to work with NW Employers to develop a programme which will include a review of the	Jane Collier / CMT / HOS TBC	Work on refreshing the strategic narratives and the values framework

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
		programme. In addition, it is felt that the 'one size fits all' competency framework is not appropriate for Managers and operational staff. HR have already started to work with North West Employers (NWE) to develop a programme which will in the first instance look at refreshing the strategic narrative, followed by the values framework.	current strategic narrative and values framework, with a view to exploring the possibility of introducing further levels of competency for managers and operational staff.		has been put on hold pending the recruitment of a new Chief Executive.
Member Code of Conduct	C/F 2020/21	Following the recent refresh of the Local Government Act's 'model Code of Conduct', Wyre's code has been benchmarked, refreshed and approved by Full Council. Following this training (Members Behaving Badly) was provided by an external party to Elected Members on the 3 February 2022. However not all Elected Members attended. In addition, following the CPSL review, Central Government responded to the review making a number of observations and recommendations for Local Authorities to consider. It is understood the Monitoring Officer (MO), Deputy MO, Head of Governance and Business Support and Democratic Services have met to consider the document and a number of actions are in the process of being actioned.	It is recommended that all Elected Members who were not able to attend the Members Behaving Badly Training are sent the video recording and handouts and certify that they have read and understood the content. In addition, consideration needs to be given to including similar training to newly Elected Members in May 2023.	Democratic Services Immediately Monitoring Officer / Deputy Monitoring Officer May 2023	Completed A similar training session to 'Members Behaving Badly' will be presented to all newly Elected Members on the 18 May 2023.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
Staff Inductions / Training and Development	C/F 2020/21	Whilst the council already has an effective corporate induction process in place, it is in the process of modernising this with the rollout of a e-learning platform 'Learning Pool'. Whist the new training platform went live in September 2021, work has stalled owing to the lack of resources within Human Resources. It is understood the new induction package will also include a number of mandatory training courses (Data Protection / GDPR and cyber security) which can also be used to refresh existing staff who have not received any data protection training since 2018 and perhaps may never have received any cyber security training.	Following the purchase of Learning Pool, the training package needs to be developed and rolled out to all new starters via the induction process. In addition, the Data Protection / GDPR and cyber security modules needs to be rolled out to all existing staff as refresher training.	Jane Collier / Marc Whittaker Joanne Billington / Lee Brophy December 2022	Learning Pool is now being used as part of the Corporate Induction process. Cyber Security and Data Protection both feature as mandatory modules and should be completed on the first day. The cyber security module is currently in the process of being completed by all existing staff. Completion rates are being monitored by HR and the Information Governance Group. Once this module has been fully completed the data protection module will then be rolled out.
Performance	C/F 2020/21	A performance audit in January 2020 highlighted that the council's processes to monitor the performance of the projects	A fundamental review of the business plan and the process for monitoring and	Marianne Hesketh / Dawn Allen	Work will commence following the business planning

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
		within the council's Business Plan require further enhancement. A new role was created, following which in June 2021 an Audit, Risk and Performance Lead was appointed to lead on the refresh of monitoring the performance of the projects within the Business Plan. Quarterly monitoring of the projects / measures within the business plan continue to be reported to CMT and Overview and Scrutiny and work is on-going to improve the processes / indicators / measures in place to monitor the performance of the council's key projects. A decision has been made to leave the fundamental review until the council starts pulling together the new business plan for 2023.	reporting key projects will be carried out, starting in January 2023 prior to pulling together the new four year Business Plan.	April 2023	session with CMT / HOS on the 15 November 2022.
Performance Appraisals	C/F 2020/21	Whilst there are standardised documents for documenting performance appraisals, it has been established that although CMT have conversations that mirror the standardised documentation these discussions are not documented on the same corporate paperwork.	To ensure a consistent approach is established, all CMT need to use the corporate performance appraisal documentation to record their 1-2-1 discussions with the Chief Executive. The NWE programme will support this change with higher-level competencies with SLT.	HR / CMT April 2023 CMT April 2023	The work required on the higher-level competences has been paused pending the appointment of a new CEX. The use of the corporate paperwork for the three Directors will be reviewed following the recruitment of the new CEX.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Progress as 1 November 2022
VFM Indicators	2021/22	During the pandemic, the value for money (VFM) indicators were not reviewed as normal and presented to Cabinet and the Overview and Scrutiny Committee.	Consideration needs to be given to the validity of running the benchmarking VFM indicators during the Covid year 2021/22.	Clare James	The benchmarking VFM report will not be produced owing to 21/22 still being impacted by the pandemic. Other benchmarking such as CIPFA's Financial Resilience Index will be used instead.

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	15 November 2022

Annual Review of Financial Regulations and Financial Procedure Rules

1. Purpose of report

1.1 To review the Financial Regulations and Financial Procedure Rules.

2. Outcomes

2.1 Evidence that the council has arrangements in place to maintain a sound system of internal control.

3. Recommendation

3.1 Members are asked to note the proposed changes summarised in paragraph 5.1 and to approve the updated Financial Regulations and Financial Procedure Rules set out in Appendix 1 of this report which can be viewed on the council's website at:

https://wyre.moderngov.co.uk/documents/b5648/Proposed%20Financial%20Regulations%20and%20Financial%20Procedure%20Rules%2015th-Nov-2022%2018.00%20Audit%20Committee.pdf?T=9

4. Background

4.1 The Financial Regulations and Financial Procedure Rules form part of the council's governance structure and help to demonstrate that arrangements are in place to maintain a sound system of internal control.

4.2 The Financial Regulations and Financial Procedure Rules were subject to a major review and updated in accordance with best practice and guidance issued by the Chartered Institute of Public Finance and Accountancy (CIPFA) prior to being agreed by the Standards Committee at their meeting on the 14 October 2004 and the Council meeting on 11 November. In addition an annual review is completed by the Head of Governance and Business Support and the Procurement Officer and reviewed by the Corporate Director Resources. The last review was completed in November 2021.

5. Key Issues and proposals

5.1 A number of amendments are proposed, namely:

- Amended to reflect the correct tile of the Corporate Director Communities (Part 4.06.03/1);
- Amended to reflect the correct title of the Risk Management Policy (Part 4.06.04/1-2. Para 3.02 and Para 3.04);
- Amended to reflect an update to the anti-money laundering legislation (Part 4.06.04/7 Para 3.47g);
- Amended to reflect the correct title of the Computer Use Policy and User Agreement (Part 4.06.04/8 Para 3.57f);
- Amended to reflect the increase in limits from £200 to £250 in relation to inventories and write-offs (Part 4.06.04/10);
- Amended to reflect that the agreed higher limits of up to £10,000 are for 'self-authorising' of goods and services (Part 4.06.05/8);
- Amended to include a further exemption to the contract procedure rules where another public authority has, in the last twelve months, procured the same or predominately similar goods, works or services (Part 4.06.07/3);
- Updated to include the requirements to be followed when procuring a new ICT system (Part 4.06.07/4);
- Update the procurement thresholds (Non-European or Lottery Funded Contracts) which came into effect from January 2022 and amend to reflect that contract values are 'inclusive of VAT' not 'net of VAT' (Part 4.06.07/4);
- To introduce a new financial limit to which all new supplier / contractor engagements, including the signing of contracts, must be approved by a second officer if signed below Head of Service or Legal Services Manager level (Part 4.06.07/9);
- Updated to include the new requirement to complete a 'Contractor / Lease Due Diligence and File Checklist' prior to contract award (Part 4.06.07/9);
- Inclusion of a new Appendix 3 - Contractor / Lease Due Diligence Checklist;
- Updated to include the new requirement to complete a 'Contractor / Lease Due Diligence Checklist' upon the receipt of a

request for an extension to a contract (Para 4.06.07/18); and

- A number of other minor amendments have been made throughout the document to correct typo's, grammar etc. These are track changed for reference.

Financial and legal implications	
Finance	None arising directly from the report.
Legal	The adoption of clear and up to date advice should ensure legal probity and good governance of the council.

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 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
Joanne Billington	01253 887372	joanne.billington@wyre.gov.uk	11.10.22

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

List of appendices

Appendix 1 – Proposed changes to Financial Regulations and Financial Procedural Rules (published on web site).

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	15 November 2022

ANNUAL REVIEW OF THE COUNCIL'S COUNTER FRAUD POLICIES – ANTI-FRAUD, CORRUPTION AND BRIBERY, ANTI-MONEY LAUNDERING, WHISTLEBLOWING AND GIFTS AND HOSPITALITY AND REGISTERING INTERESTS

1. Purpose of report

1.1 Approval of the Council's Counter Fraud Policies, namely:

- Anti-Fraud, Corruption and Bribery;
- Anti-Money Laundering;
- Whistleblowing; and
- Gifts and Hospitality and Registering Interests.

2. Outcomes

2.1 The ability to demonstrate that the council has arrangements in place that are designed to promote and ensure probity and propriety in the conduct of its business.

3. Recommendation

3.1 Members are asked to approve the revised policy documents detailed above at paragraph 1.1.

4. Background

4.1 The council is determined to do everything it can to reasonably deter fraud, corruption and bribery across all areas of council activity. It works hard to encourage the detection, reporting and investigation of fraud and actively promotes a zero tolerance approach.

4.2 Counter fraud covers not just fraud threats from inside and outside of the organisation, but is also linked to areas like bribery, corruption and money laundering. The council has four main counter fraud polices which assists the organisation in maintaining and developing an effective counter fraud culture. They are as follows;

- Anti-Fraud, Corruption and Bribery;

- Anti-Money Laundering Policy and Procedure;
- Whistleblowing; and
- Gifts and Hospitality and Registering Interests.

4.4 The general aim of these policies is to reduce the occurrence and impact of fraud, corruption and bribery on the organisation and provide an effective channel of communication for anyone who has concerns or suspicions of malpractice.

4.5 The Audit Committee work programme allows for an annual review of all the above policies, with the last review being completed in November 2021.

5. Key Issues and proposals

5.1 The Anti-Fraud, Corruption and Bribery Policy has been amended as follows:

- to reflect the correct titles of the ICT Service Desk Computer Use Policy and User Agreement and the council's Complaints, Feedback and Compliments Procedure;
- to include reference to the 'ethical governance survey' that is used to test the council's knowledge of its counter fraud polices;
- to reflect that any suspicions of fraud, corruption or bribery concerning Elected Members should be directed to the Monitoring Officer;
- to include the requirement to ensure compliance with the council's Financial Regulations and Financial Procedure Rules;
- to refer to a new procedure within the Revenues and Benefits Section - 'inappropriate use of revenues and benefit software declaration' (Appendix B), and;
- to update the 'Seven Principles of Public' Life (Appendix C) to accurately reflect the wording set out by the Nolan Committee.

5.2 The Anti-Money Laundering Policy and Procedure has been amended as follows:

- to reflect the recent changes to UK anti-money laundering legislation which came into force on the 1 September 2022;
- to encourage staff to raise any concerns through the Money Laundering Reporting Officer or through the appropriate whistleblowing channels;
- to reflect updated guidance on 'submitting better quality suspicious activity reports' to the National Crime Agency, and;
- to amend the 'additional guidance' section to include updated money laundering legislation and guidance and details for the Public Interest and Disclosure Act 1998.

5.3 The Whistleblowing Policy has been amended as follows:

- to reflect that the council will do its best to protect the identity of the whistlblower 'indefinitely' if applicable;
- to reflect that the council will avoid wherever possible referring to

the fact a whistleblowing has triggered an investigation;

- to confirm that the whistleblower can raise a concern through whichever channel they find most appropriate;
- to provide assurance that all concerns (no matter how small) are logged and examined to determine any necessary action and build up a picture;
- to introduce a reporting channel to follow if the user feels their concerns have not be addressed satisfactorily;
- to reflect that investigations may be carried out by an external organsiation to address conflicts of interest and protect internal officers;
- to set out the requirement to follow-up on any agreed actions;
- to document the requirement to appoint a 'key point of contact';
- to include the requirement to complete a 'lessons learnt' exercise following each investigation to ensure the policy is still fit for purpose, and;
- to document the methods used by the council to review the effectiveness of this policy.

5.4 The Gifts and Hospitality and Registering Interest's Policy has been amended to reflect that if gifts are received from the same source which cumulatively, are over the value of £25 in a 12 month period, then these must be declared and the officer should seek authorisation from their manager or their Corporate Director.

5.5 The amended draft policies can be viewed at the following link. All amendments have been track changed.

https://wyregovuk.sharepoint.com/sites/Councillor-Portal/SitePages/Counter-fraud-and-corruption.aspx

Financial and legal implications	
Finance	There are no specific financial implications arising from the adoption of these counter-fraud policies.
Legal	The Council's counter-fraud policies assist in good governance and probity of council actions and decision-making.

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

risks/implications	**✓ / x**
asset management	X

equality and diversity	X
sustainability	X
health and safety	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
Joanne Billington	01253 887372	joanne.billington@wyre.gov.uk	31.10.2022

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

List of appendices

None

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	15 November 2022

ANNUAL REVIEW OF THE COUNCIL'S INFORMATION GOVERNANCE POLICIES AND PROCEDURES – DATA PROTECTION POLICY AND PROCEDURE, RECORDS MANAGEMENT POLICY AND SUBJECT ACCESS REQUEST PROCEDURE

1. Purpose of report

1.1 Approval of the council's information governance policies and procedures, namely:

- Data Protection Policy and Procedure;
- Records Management Policy, and;
- Subject Access Request Procedure.

2. Outcomes

2.1 The ability to demonstrate that the council has robust data governance arrangements in place that are designed to establish a set of rules and procedures, ensuring data accuracy, reliability, compliance and security.

3. Recommendation

3.1 Members are asked to approve the revised policies and procedures detailed at paragraph 1.1.

4. Background

4.1 The goal of a robust information governance framework is to make all council information (information assets) available when needed, hold it in a safe location, while reducing storage costs, ensuring compliance to external legislation and internal policy and procedures. There are many benefits of having an effective information governance framework in place, however the main benefits are as follows:

- assist in making data consistent;
- improves data quality;
- assists with data accuracy, ensuring it's fit for purpose;
- improves business planning and decision making; and
- reduces the chances of a serious data incident.

4.2 Information governance polices are also important because they provide a framework to staff to ensure that all information is dealt with consistently legally, securely, efficiently and effectively.

4.3 The Audit Committee's Terms of Reference (Part 2 Article 7), states they are to receive updates and reports from the Head of Governance and Business Support (Data Protection Officer) and to approve policies in relation to cyber security and compliance to the Data Protection Act as well as Regulations made under the Act; namely the UK GDPR. In addition, the committee's work programme allows for an annual review of all policies named at paragraph 1.1.

5. Key Issues and proposals

5.1 The council's Data Protection Policy was last reviewed by the Audit Committee in November 2021. The policy has had a number of changes which have been tracked throughout the document. Once approved, this policy will be made available to the public via the council's website.

5.2 The Records Management Policy has never previously been presented to the Audit Committee for formal approval. It was last refreshed in 2012 prior to the General Data Protection Regulations which came into force on 25 May 2018. Therefore, the previous policy required a fundamental review and rewrite. There are no track changes to this document. This policy is only available to council officers on the HUB under the information governance section.

5.3 The Subject Access Request Procedures have never previously been presented to the Audit Committee for approval. Whilst the Information Commissioner's Office (ICO) and the Data Protection Act 2018 and UK GDPR instructs on the handling of SAR's, the council has in addition produced internal guidance to assist officers in the administration of these. This guidance is only available to council officers on the HUB under the information governance section.

5.4 The draft policies for approval can be found at Appendices 1, 2 and 3.

Financial and legal implications	
Finance	There are no specific financial implications arising from the adoption of these information governance policies.
Legal	The council's information governance policies assist the council in complying with a number of external regulations in relation to data protection, records management and meeting the rights of data subjects.

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	✓
Data protection	✓

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
Joanne Billington	01253 887372	joanne.billington@wyre.gov.uk	01.11.2022

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

List of appendices

Appendix 1 – Data Protection Policy and Procedures

Appendix 2 – Records Management Policy

Appendix 3 – Subject Access Request Procedure

This page is intentionally left blank

Appendix 1

Formatted: Font: Bold

Data Protection Policy and Procedures

Version 43.0 – November 20221

1.0 Introduction

1.1 The processing of personal data is essential to many of the services and functions carried out by local authorities. Wyre Council ('the cCouncil') recognises that compliance with data protection legislation (including the UK General Data Protection Regulations ('GDPR'), the Data Protection Act 2018 ('DPA') and related legislation) will ensure that such processing is carried out fairly, lawfully and transparently.

1.2 Data protection legislation and Article 8 of the European Convention on Human Rights recognise that the processing of personal data needs to strike a balance between the need for an organisation utilising personal data to function effectively, efficiently and in the wider public interest, and respect for the rights and freedoms of the individual(s) ('data subject(s)') to whom the personal data relates. This policy sets out how the cCouncil intends to safeguard those rights and freedoms.

1.3 The Information Commissioner's Office (ICO) is an independent authority which has legal powers to ensure organisations comply with the DPA and UK GDPR. For more information on the role of the ICO, please go to www.ico.org.uk.

2.0 Scope

2.1 This policy applies to the collection, use, sharing and other processing of all personal data held by the cCouncil, in any format including paper, electronic, audio and visual. It applies to all council staff. 'Staff' for the purposes of this policy includes all council officers, volunteers and agency staff. Council contractors are covered under their own terms and conditions. Paragraph 9.3 provides further details.

3.0 Legal context

3.1 Reference to the following legislation and guidance may be required when reading this policy.

- The Data Protection Act 2018
- The UK General Data Protection Regulations
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998

3.2 Reference to the following internal council documents may also be required when reading this Policy;

- The cCouncil's Constitution

- Employee's Code of Conduct
- ICT Service Desk Computer Use Policy and User Agreement
- Security Incident Policy
- Records Management Policy ~~(in review)~~
- Password Policy and User Guidance

4.0 Personal data processed by the c~~C~~ouncil

4.1 The c~~C~~ouncil processes personal data for many reasons, including in relation to the services it provides and in its role as an employer. In most instances the c~~C~~ouncil will be the data controller (usually alone, but sometimes jointly) in respect of the personal data it processes (i.e. it will determine the purpose and means of the processing); on occasion it may act as a data processor on behalf of another data controller.

4.2 Whether acting as a data controller in its own right, or on another's behalf as data processor, the c~~C~~ouncil will maintain a record of its processing activities and make this available to the Office of the Information Commissioner ('ICO') upon request. Information concerning the processing of personal data in respect of which the c~~C~~ouncil is a data controller will be communicated by the c~~C~~ouncil to data subjects by means of appropriate privacy notices.

4.3 The c~~C~~ouncil has an overarching privacy notice and individual service privacy notices that can be found on the c~~C~~ouncil's website.

4.4 The c~~C~~ouncil is committed to ensuring compliance with data processing legislation and will:

- Respect the rights of each individual;
- Be open and honest about the personal data it holds;
- Provide training and support to those handling personal data in the course of their duties;
- Notify the ICO annually, that it processes data. This is a statutory requirement and notification must be kept up to date with any changes to the use of personal data being updated within 28 days. (The c~~C~~ouncil has two registration numbers Z5682712 (General processing) and ZA319367 (E~~e~~lected Members) and;
- Inform the ICO and in some instances the data subject of any data breaches.

5.0 Data protection principles

5.1 The c~~C~~ouncil will comply with the principles relating to the processing of personal data set out in the UK GDPR by putting in place processes to ensure that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject) and;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 The cCouncil shall be responsible for, and be able to demonstrate compliance with all the above principles.

5.3 Where the cCouncil processes personal data as a 'competent authority' for 'law enforcement purposes' (i.e under statutory law enforcement functions) it shall do so in accordance with the version of the data protection principles set out in the Law Enforcement provisions of the DPA. Those principles are similar (but not identical) to the principles applying to more general processing of personal data detailed above.

5.4 'Law enforcement purposes' include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety.

6.0 Legal basis for processing

6.1 The cCouncil will ensure that it's processing of personal data (other than law enforcement processing) fulfils the appropriate general condition(s) for processing outlined in the UK GDPR. Where a 'special category' of personal data is processed (this includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of identifying an individual, physical or mental health, sex life or sexual orientation), the cCouncil will

ensure that one of the additional conditions set out in relation to special category personal data in the UK GDPR is also met, along with any further requirements regarding the processing of sensitive personal data set out in other data protection legislation.

6.2 While not formally defined as a 'special category' of personal data under the UK GDPR, similar additional conditions and requirements also apply to personal data relating to criminal convictions and offences (including personal data relating to the alleged commission of offences and proceedings relating to the commission or alleged commission of offences). When processing such data the cCouncil will ensure that the relevant additional conditions and requirements are met.

6.3 Where the council processes personal data as a 'competent authority' for 'law enforcement purposes' it shall do so in accordance with the requirements of the law enforcement provisions of the DPA. In all cases such processing will only be carried out where the individual concerned has given their consent to the processing of their personal data for law enforcement purposes or where the processing is necessary for the performance of a task carried out for law enforcement purposes by a competent authority. Where such processing involves 'sensitive processing' (this is equivalent to the processing of special category personal data under the UK GDPR) the cCouncil will ensure that the processing is strictly necessary and (unless the individual has consented to the processing) that one of the conditions for sensitive processing set out in the DPA is met.

7.0 Individuals' rights

7.1 Data protection legislation provides individuals with various rights. An individual's rights include:

- The right to be provided with specified information about the cCouncil's processing of their personal data **('the right to be informed').**
- The right to access their personal data and certain supplementary information **('the right of access').**
- The right to have their personal data rectified, if it is inaccurate or incomplete **('the right of rectification').**
- The right to have, in certain circumstances, their personal data deleted or removed **('the right of erasure', sometimes knowns as 'the right to be forgotten').**
- The right, in certain circumstances, to restrict the processing of their personal data **('the right to restrict processing').**
- The right, in certain circumstances, to move personal data the individual has provided to the cCouncil to another organisation **('the right of data portability').**

- The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the cCouncil to stop processing that data **('the right to object').**

- The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing **('Rights related to automated decision making, including profiling').**

7.2 In relation to the first right referred to above ('the right to be informed') in general the cCouncil will:

- where the personal data is collected from an individual, provide them with specified privacy notice information, at the time the personal data is collected, for example when a member of the public is signing up to receive a council service;

- where the personal data has not been obtained from an individual, provide them with specified privacy notice information within one month; if the cCouncil uses personal data that it has not collected directly from an individual to communicate with that individual, it will provide the specified privacy notice information, at the latest, when the first communication takes place; if disclosure to another recipient of personal data, that has not been collected directly from the individual is envisaged, the cCouncil will provide the specified privacy notice information, at the latest, before the data is disclosed.

7.3 It should be noted that there are limited specified circumstances in which the right to be informed will not apply. For further information go to www.ICO.org.uk

7.4 Where an individual exercises one of the other rights listed above, the cCouncil will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:

- Where further time is necessary, taking into account the complexity and the number of the request(s) from the data subject, the period for responding will be extended by up to two further calendar months. Where such an extension is required the cCouncil will notify the data subject that this is the case within one calendar month of receiving their request.

- Where the request(s) from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character) the cCouncil will ordinarily refuse the request(s). In exceptional cases the cCouncil may instead exercise its alternative right in such

circumstances to charge a reasonable fee that takes into account the administrative cost of complying with the request.

7.5 The cCouncil recognises the fundamental nature of the individual rights provided by data protection legislation. The cCouncil will ensure that all valid requests from individuals to exercise those rights are dealt with as quickly as possible and by no later than the timescales allowed in the legislation.

7.6 To minimise delays, and to help ensure that the cCouncil properly understands the request being made, it is preferable for requests from data subjects wishing to exercise their data subject rights to be either in writing or made via the cCouncil's on-line process. However, a valid request may also be made verbally.

7.7 The cCouncil's dedicated email address for exercising individual rights is informationgovernance@wyre.gov.uk or individuals can use the council's online form available from the cCouncil's website at;

https://www.wyre.gov.uk/info/200373/your_data_and_us

7.8 All requests from data subjects to exercise their data subject rights must:

- Be accompanied by, where necessary, proof of the identity of the data subject and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or authorised agent);
- Specify clearly and simply how the data subject wishes to exercise their rights – this does not mean that an individual needs to refer specifically to a particular right by name or legislative provision (for example, "I would like a copy of my employee file" is sufficiently clear to indicate that the right of access is being engaged);
- Give adequate information to enable the cCouncil to determine whether the right is engaged and to comply (subject to any exemption(s)) if it is;
- Make it clear where the response should be sent; and
- Where relevant specify the preferred format in which any information disclosed to the data subject should be provided.

7.9 Data protection law allows exemptions from complying with data subject rights in specific and limited circumstances. The cCouncil will normally apply the exemptions where they are engaged, unless it is satisfied that it is appropriate or reasonable not to do so.

7.10 If a data subject exercising one or more of their data subject rights is dissatisfied with the response received from the cCouncil, they may ask for the matter to be dealt with by the cCouncil's Data Protection Officer (DPO).

Alternatively, a data subject also has the right to complain to the ICO if they believe that there has been an infringement by the cCouncil of data protection legislation in relation to the data subject's personal data. A data subject may also pursue a legal remedy via the courts. Further information on the rights of data subjects is available from the ICO's website www.ico.org.uk.

7.11 Additional guidance for staff on how to deal with requests to exercise data subject rights is available via the cCouncil's Hub.~~intranet.~~

8.0 Individuals' Rights – Law Enforcement Processing

8.1 The rules relating to an individual's rights are different where the cCouncil processes personal data as a 'competent authority' for 'law enforcement purposes'. In those circumstances individuals have the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restriction of processing; and
- the right not to be subject to automated processing.

8.2 There are no equivalents to the right to object or the right to data portability. Also, the right of access, the right to rectification and the right to erasure or restriction of processing will not apply to 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

8.3 'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. Where an individual exercises their rights in respect of personal data that the cCouncil is processing for law enforcement purposes the cCouncil will ordinarily respond without undue delay and in any event within one calendar month. There is not an option for the cCouncil to extend this for a further period in the case of complex or numerous requests, although the cCouncil can refuse (or make an administrative charge for) manifestly unfounded or excessive requests.

9.0 Further legal requirements

9.1 The cCouncil may be required to disclose personal data to a person or organisation other than the data subject by virtue of a court order, or to comply with other legal requirements, including those relating to the prevention or detection of crime, the apprehension/prosecution of an offender, or the collection of taxation/duties.

9.2 The cCouncil may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances the cCouncil will always give proper consideration to the data subject's interests and their right to privacy.

9.3 External agencies, companies or individuals undertaking processing of personal data on behalf of the cCouncil ("data processors") must be required to demonstrate, via a written contractual agreement, that personal data belonging to the cCouncil will be handled in compliance with data protection legislation and that appropriate technical and organisational security measures are in place to ensure this. Any contractual agreement between the cCouncil and a data processor will contain all the relevant elements specified in data protection legislation.

9.4 The cCouncil will follow relevant guidance issued by the Government, the ICO and the Surveillance Camera Commissioner for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and staff have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same.

9.5 Officers must always ensure that prior to the purchasing, installing or modifying of any council CCTV system, approval and/or sign off must have been sought from the council's Partnership Officer (CCTV).

9.65 The cCouncil reserves the right to monitor telephone calls, e-mail and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO and the Investigatory Powers Commissioner's Office (IPCO).

10.0 Privacy by design and by default (Privacy Impact Assessments (PIA))

10.1 The cCouncil's approach to compliance with data protection legislation will be underpinned by the principles of privacy by design and privacy by default. 'Privacy by design' means that the cCouncil will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data.

10.2 'Privacy by default' means that the cCouncil will ensure that only personal data that is necessary for a specific purpose is processed. The cCouncil will not collect more personal data than is needed for the purposes concerned, process it more than is necessary or store it longer than is needed.

10.3 When undertaking a new activity, privacy considerations will be embedded throughout. A Privacy Impact Assessment (PIA) will need to be completed and signed off by the cCouncil's DPO before the activity commences. The Corporate Management Team should ensure that any decisions taken to implement new systems of processing are supported by a completed PIA.

11.0 Records Management

11.1 The cCouncil must manage and dispose of its records in accordance with the cCouncil's Records Management Policy (under review) and service specific Information Asset Registers. It is essential that records are stored securely and the location of information is up to date at all times to enable the cCouncil to process any requests for information (FOI's and SAR's) within the required timescales.

12.0 Information Security

12.1 Effective methods of security must be in place to help prevent the inappropriate disclosure or loss of personal data. The cCouncil will process personal data in accordance with the DPA and UK GDPR and any other related cCouncil policy and procedure to ensure appropriate physical, technical and organisational measures are in place.

12.2 Access to areas where data is stored and used must be controlled as follows:

- Paper files must be locked away when not in use and electronic systems must be password protected, with only authorised users being given access;
- Hybrid workers and other staff working away from the office must ensure records are adequately protected at all times, preventing damage, theft / loss and unauthorised access to personal data;
- Electronic data must be stored on the cCouncil's servers and should be backed up each night to prevent the loss of valuable data;
- Personal data must not be stored on unencrypted portable equipment, e.g. laptops, mobile phones, tablet devices or memory sticks / pen drives. Staff are advised to contact the ICT Service Desk for assistance if they are wanting to transfer personal data out of the organisation;
- Computers, laptops and tablet devices must be password protected and locked when left unattended during the day. Staff are required to log off and shut down all systems at the end of the working day;
- Staff must not disclose passwords to colleagues or use passwords belonging to other staff members.
- Confidential waste bins are located throughout the building and can be used for all paper disposal. However they must always be used for the destruction of personal data. The cCouncil employs a contractor to shred all paper waste on site once a week, therefore there is no requirement to shred any personal data prior to using the confidential waste bins. Hybrid workers should continue to use the office facilities provided to dispose of confidential waste and should not make their own arrangements for the removal and disposal of council data.

13.0 Information Sharing

13.1 When personal data is collected, the data subject must be informed, via a privacy notice, what data the cCouncil expects to share, with whom it is likely to be shared and in what circumstances. See 7.2 for guidance on when the data subject needs to be informed.

13.2 Non-sensitive personal data may be shared across cCouncil departments and with contractors working on the cCouncil's behalf for legitimate purposes, such as:

- Updating cCouncil records;
- Providing services; and
- Preventing and detecting fraud.

- Any sharing of personal data and the purpose for the sharing must be documented in the individual service's information asset register.

Formatted: No bullets or numbering

Formatted: Indent: Left: 0 cm, Hanging: 1.25 cm, No bullets or numbering

13.3 Sensitive personal data is normally only disclosed with the informed consent of the data subject. However, there are circumstances in which personal data may be disclosed without obtaining the data subject's consent such as when safeguarding the data subject or others, and to assist with the prevention and detection of crime. For further guidance, refer to the ICO's website or speak to the cCouncil's DPO.

13.4 Information sharing protocols / agreements should be in place between all cCouncil and third parties when personal data is being shared. All agreements must be signed off by the DPO and the council's Legal Services Manager and then details of the sharing should be documented in ~~at which point a record of the data shared will be documented in~~ the relevant information asset register by the Service Manager.

13.5 Any sharing of cCouncil-controlled personal data with other data controllers must comply with all statutory requirements and corporate policies. Where appropriate the cCouncil will enter into a data sharing agreement before sharing personal data with another data controller, particularly where personal data is to be shared on a large scale and/or on a regular basis. ~~regularly.~~ Any data sharing agreements must be signed off by the DPO and the cCouncil's Legal Services Manager.

14.0 Secure Transfer of Data

14.1 The transfer of data in all formats (written, fax, email, phone or face to face) must be completed in a secure manner, ensuring the identity of the recipient has been verified. This will help prevent personal data being misplaced or disclosed in error. Hybrid workers must take particular care when working in an unsecure location and must ensure they cannot be overheard when disclosing personal data.

14.2 Secure Email

When providing information by email, client details must not be placed in the subject heading. Be aware that when the recipient replies and includes your original email, the return email is not secure. Recipients should be made aware of this and be advised to refer to their own organisation's procedures. All emails that contain personal data must be encrypted. Password protecting the email or file is not sufficient protection to secure the contents. Employees should contact ICT Service Desk if they do not know how to encrypt an email or a document that contains personal data.

14.3 Postal Mail
The cCouncil has a data classification scheme in place that sets out how internal and external mail should be sent depending on its content.

14.4 Fax
When sending personal data by fax, it is imperative that the sender phones ahead to the receiver to ensure they are standing by the machine to receive the fax. The receiver must then confirm that the fax has been received in full.

15.0 Roles and Responsibilities

15.1 Everyone representing the cCouncil has a duty to protect the information it holds and access to personal data must be on a strict need to know basis. Personal data must not be disclosed without appropriate authorisation.

15.2 The cCouncil has an Information Governance Group which is accountable for ensuring compliance with this policy across the cCouncil. The work of the group will be supported by the Corporate Management Team (which includes the council's SIRO) and the Audit Committee who have delegated responsibility for ensuring the cCouncil's compliance to the DPA and UK GDPR. The group's primary membership consists of the DPO, the Information Governance Manager (Deputy DPO), ICT Services Manager ~~Delivery Lead, and the~~ Legal Services Manager and the Legal Executive. However, other officers are also invited to attend, depending on the agenda. All meetings have a structured agenda, are minuted with agreed actions being allocated to a specific officer with an agreed timescale. These minutes are provided to CMT as part of the Head of Governance and Business Support's quarterly update.

15.3 The cCouncil will ensure that:

- ~~The~~ The DPO reports to the highest management level of the cCouncil in respect of their duties as DPO, in this instance, this is the Senior Information Risk Owner (Chief Executive) who forms part of the Corporate Management Team.; ~~and reports are submitted on a quarterly basis.~~
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Individuals handling personal data will be trained to an appropriate level in the use and control of personal data.
- All staff handling personal data know when and how to report any actual or suspected data breach, and that appropriately trained staff manage any breach correctly, lawfully and in a timely manner.
- Breaches will be reported to the ICO where such reporting is mandatory or otherwise appropriate and shall be done within the required timescales.
- It monitors and reviews its processing activities to ensure these are compliant with data protection legislation.

- Where there is any new or altered processing of personal data it will take appropriate steps (including where necessary a privacy impact assessment) to identify and assess the impact on data subjects' privacy as a result of the processing of their personal data.
- Appropriate privacy notices are maintained to inform data subjects of how their data will be used and to provide other mandatory or relevant information.
- This policy remains consistent with the law, and any compliance advice and codes of practice issued from time to time by the ICO is incorporated.

15.4 Elected Members may have access to, and process personal data in the same way as employees and therefore must comply with the six data protection principles. These can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/

15.5 As data held on c~~C~~ouncil systems may be used by Elected Members in their roles, the data controller may be the Elected Member or the c~~C~~ouncil individually, jointly or on behalf of the other. Notification must be arranged as follows:

- When acting on behalf of the c~~C~~ouncil, Elected Members can rely on the c~~C~~ouncil's legal basis and notifications for processing.
- When acting on their own behalf, for example, when dealing with complaints made by local residents, Elected Members are data controllers in their own right, therefore must themselves ensure they comply with the DPA and the UK GDPR.
- When campaigning within their own political party (unless Independent Members), Members may rely on the legal basis and notification for processing of their own party.

15.6 From ~~the~~ 1 April 2019, the requirement for Elected Members to pay a registration fee to the ICO was abolished. Elected Members are now exempt from paying a fee, unless they process personal data for purposes other than the exercise of their functions as an Elected Member. For example, if they have their own business or they are using CCTV for business or crime prevention purposes in connection with that business, then a fee will still apply.

15.7 Whilst the majority of the c~~C~~ouncil's Elected Members will be exempt from paying a fee and having to register with the ICO, they are still Data Controllers in their own right and therefore have data protection responsibilities. This means they are responsible for making sure all personal data handled complies with the requirements of the DPA and UK GDPR. All Elected Members have been issued with guidance on how they can achieve this. They have also been provided with a privacy notice which they can distribute to their constituents.

15.8 The DPO will arrange periodic data protection training for the council's Elected Members, which they must attend. They must also follow any advice and guidance provided to them ~~all training recommended to them~~ and take the necessary steps to ensure the c~~C~~ouncil's data is stored safely in accordance with any c~~C~~ouncil policy and procedure. They must store all c~~C~~ouncil data separately from data relating to their ward and political party work.

16.0 Training

16.1 The c~~C~~ouncil recognises that data protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution.

16.2 All data protection training provided by the c~~C~~ouncil is mandatory and Line Managers are responsible for ensuring that all staff are given the necessary time to participate. At present, the c~~C~~ouncil provides all new starters with an induction pack which includes the Data Protection Policy and Procedures and Incident / Breach Reporting and Investigation Instruction. ~~All~~ In addition, all new starters are asked to complete a mandatory cyber security and data protection training module in the council's e-learning training portal (Learning Pool). They are provided with the council's Computer Use Policy and User Agreement and are then required to complete a 'user declaration' to confirm they have read and understood the Policy. This declaration is retained on their personnel file. ~~staff are asked to sign to confirm they have read and that they understand the content of both documents. The Council has recently procured an e-learning training portal (Learning Pool) which launched in September 2021. From January 2022 it will be the primary tool used to train all staff on data protection and information security~~. All existing staff will be required to complete both the mandatory cyber security and data protection training modules every two years.

16.3 Some post-holders are required to undertake further information governance or data protection training where appropriate for a particular role or within a specific service area, for example the DPO and their deputy and staff with specific responsibility for processing Freedom of Information (FOI's) Act requests and Subject Access Requests (SAR's).

17.0 Reporting a potential data breach

17.1 In the event of a suspected data breach it is essential that staff follow the guidance for reporting potential breaches (attached at Appendix A). Adhering to this guidance will ensure that all risks are identified and mitigated, the appropriate people and organisations are informed, and communication is prepared to help prevent damage to the data subject and the c~~C~~ouncil's reputation.

17.2 All incidents, including near misses, should be reported to the DPO or the Deputy DPO. Failure to report an incident could result in disciplinary action including dismissal (see 19.1).

17.3 All incidents are logged into a 'data incident log' which is maintained by the DPO and monitored by the Information Governance Group. It is also available for inspection by the ICO.

17.4 It should be noted that at present, the council has a separate 'Security Incident Protocol' for the reporting and recording of any ICT related incidents, e.g. loss of equipment, viruses, bogus emails etc. However, this protocol does not supersede the guidance attached at Appendix A.

18.0 Governance and Distribution

18.1 The ownership of this policy sits with the Information Governance Group. The group will review the policy annually with any changes being submitted to the Audit Committee for approval.

18.2 The policy will be displayed on the cCouncil's Hub~~intranet~~ and also the cCouncil's website on the data protection web page:

https://www.wyre.gov.uk/info/200373/your_data_and_us

19.0 Disciplinary action and criminal offences

19.1 Serious breaches by staff of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action including dismissal and may even give rise to criminal offences.

20.0 Sources of information and guidance

20.1 This policy is supported by training, awareness and additional guidance made available to staff on the cCouncil's Hub~~intranet~~. The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of information law for use by organisations and the public. Please see www.ico.org.uk

20.2 Other useful contact details

Data Protection Officer	01253 887372
Deputy Data Protection Officer	01253 887503
Legal Services Manager	01253 887214
Information Commission Officer helpline	0303 123 1113
ICT Service Desk~~helpdesk~~	01253 887652

Appendix A

Incident / breach reporting and investigation instruction

1.0 Introduction

1.1 Wyre Council is obliged under Data Protection law to investigate any breaches of security that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data when it is being used in any content or location.

1.2 The organisation needs to take steps as quickly as possible to recover any data involved in the incident or otherwise contain the spread or effects of the incident, whilst trying to ensure that the cause of the incident is properly identified. At Wyre Council, this responsibility falls to the Data Protection Officer (DPO) or the Deputy DPO.

1.3 Once an incident comes to light, a decision must be made by the DPO or their Deputy within 72 hours about whether to inform the Information Commissioner, and subsequently, whether to inform the affected individuals.

1.4 A genuine accident, mistake or theft that could not have been prevented is not considered to be a breach of Data Protection law, whereas a failure to implement proper security measures, whether technical or practical, to protect data is almost certainly a breach. Either way, they both need to be reported to the DPO or their Deputy and investigated thoroughly.

2.0 What to look out for and what should I report?

2.1 Losses and theft

- Loss or theft or paper documents / equipment containing council / personal data, especially sensitive or confidential information;
- Unauthorised access to, tampering with or use of ICT systems or equipment;
- Unauthorised changes to system hardware, firmware or software; or
- A deliberate attempt by a third party to steal data.

2.2 Mishandling

- Emails, post, faxes or other correspondence sent to the wrong person or destination, especially where the data is sensitive or the incidents are repeated;
- Wrong data or files attached to correspondence when sent out;
- Data or equipment on which data is stored is not securely disposed of; or
- Data or equipment is left in vacated buildings or furniture containing records is disposed of without records being cleared out.

2.3 Improper and inappropriate use

- Improper use of ICT system;
- Use of non-work email, equipment or storage for work purposes; or

- Failure to revoke access from leavers, contractors or people changing job roles.

2.4 Electronic and operational

- Malware attacks (viruses, ransomware, worms, Trojan horses);
- Unauthorised disruption of service, phishing attacks etc., or;
- System failure, crashes, environmental failures and operator errors. These may have security implications and should be treated as incidents.

3.0 How should I report one of the above?

3.1 Any suspected data breaches must be reported immediately in the first instance to the DPO or Deputy DPO. In the instance that neither officer is available, your Director or Service Manager should be informed. Contact details for the DPO and the Deputy DPO are as follows;

Data Protection Officer	Joanne Billington	01253 887372
Deputy Data Protection Officer	Joanne Porter	01253 887503

Alternatively, you can email the cCouncil's dedicated incident reporting mailbox informationgovernance@wyre.gov.uk

3.2 Given that the organisation has a responsibility to notify the ICO where applicable within 72 hours of the identification of a breach, it is imperative that officers report incidents immediately, to allow the 72 hour timescale to be adhered to.

3.3 All documentation in relation to the incident must be collated and held securely until further instruction is given by the DPO or Deputy DPO. The DPO or Deputy will ask you for a 'written statement of fact'. Which is basically a detailed account of how the incident occurred, what data has been lost or put at risk and any other information that is important to the investigation.

3.4 It should be noted at this stage, any investigation is carried out in an informal manner with the primary objective being to ascertain if an 'actual breach' has occurred and if the breach has or could cause harm or damage to an individual or the organisation.

3.5 Staff under no circumstances should alert the data subject, the ICO or any third party to the suspected incident. The decision to notify the individuals concerned, the ICO and any third parties is the responsibility of the DPO or the Deputy DPO following a full investigation.

3.6 Failure to report an incident or adhere to paragraphs 3.1 – 3.5 above could lead to disciplinarily action.

4.0 Management of a data breach / incident

4.1 Once it has been identified that an actual data breach has occurred, it is important that the cCouncil has an effective, documented plan of how they will deal with the incident. The DPO or the Deputy DPO is responsible for

ensuring that all reported incidents are dealt with as quickly as possible, in a transparent and consistent way.

4.2 As part of the investigation, the DPO or Deputy DPO will take the following four steps;

- Containment and Recovery
- Assessment of Risks
- Notification
- Evaluation and Response

4.3 The DPO or Deputy DPO may ask for your involvement at any stage of the investigation and it is expected that full participation and cooperation will be given. Where it is deemed that deliberate obstruction or withholding of information is taking place, this may lead to the council taking disciplinary action.

Records Management Policy

Version 2.0 – November 2022

1.0 Purpose of this policy

1.1 This document sets out the council-wide policy for records management standards that should be adhered to by all staff working with Wyre Council (the council) records.

1.2 All employees of the council have a responsibility to effectively manage council records and manage them appropriately in a way that meets the council's legal obligations.

2.0 Introduction

2.1 Any evidence of council business activity is a record. Records, therefore can be paper documents, electronic files, emails, databases, maps or images.

2.2 Records are the council's corporate memory and provide the evidence of its business actions and decisions. They also provide evidence that the council has satisfied statutory requirements. Well-managed records can improve the process of decision-making and facilitate business administration. They are, therefore, a corporate asset.

2.3 A record is a piece of information that has an intrinsic worth, which makes it important enough to save and keep secure for its evidential value. In order to decide whether a piece of information is a record or not, its business context must be understood as well as its relevance and significance to the organisation. If a record is of value as evidence of business activity, it is important that it be managed in a way that ensures the record:

- can be easily and quickly retrieved;
- is authentic - it is what it purports to be;
- is reliable - information in the record is accurate and can be depended on;
- has integrity – it is complete and unaltered;
- has appropriate context information about where it was used and why; and
- has structure so that the record is intact.

3.0 Relevant legislation

3.1 The council is committed to continuously improving the way it responds to requests for information under statutory access regimes. This includes the Freedom of Information (FOI) Act 2000, the Data Protection Act (DPA) 2018, the UK General Data Protection Regulation (UK GDPR) and the Environmental Information Regulations (EIR) 2004. Compliance however, is reliant upon proper management of the council's information, which needs to be managed, stored securely and easily located.

3.2 The DPA and the UK GDPR requires all organisations that handle personal information to comply with six principles regarding privacy and disclosure. Particularly relevant to records management is the fifth principle, which states that “Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”.

3.3 The Local Government (Records) Act 1962 gave local authorities limited discretionary powers to hold their records in local archives. In particular, it states that “A local authority may do all such things as appear to it necessary or expedient for enabling adequate use to be made of records under its control”.

3.4 The Local Government Act (LGA) 1972 sets out the basic requirement for local authorities to ‘make proper arrangements’ to keep good records.

3.5 Reference to the following legislation and guidance may also be required when reading this policy.

- Computer Misuse Act 1990
- Human Rights Act 1998
- Public Records Act 1958 and 1967
- Local Government (Access to information) Act 1985
- Records Management Standards and guidelines British Standards (BSI)
- Lord Chancellors’ Code of Practice on Management of Records issued under S.46 of the Freedom of Information Act 2000

3.6 This list is not exhaustive and there will be other record-keeping legislation specific to certain areas of work, which should also be taken into account.

3.7 Reference to the following internal council documents may also be required when reading this Policy;

- The Council’s Constitution
- Employee’s Code of Conduct
- ICT Service Desk Computer Use Policy and User Agreement
- Security Incident Policy
- Data Protection Policy
- Data Classification Scheme
- Password Policy and User Guidance

4.0 Objectives

4.1 The aim of this policy is to define a framework for managing the council’s records to ensure that the council:

- creates and captures accurate, authentic and reliable records;
- maintains records to meet the authority’s business needs;

- disposes of records that are no longer required in an appropriate manner;
- protects vital records;
- conforms to any legal and statutory requirements relating to record keeping, retention and disposal; and
- complies with government directives.

4.2 Whether acting as a data controller in its own right, or in common, or on another's behalf as a data processor, the council will maintain a record of its processing activities and make this available to the Information Commissioner's Office (ICO) on request. Information concerning the processing of personal data in respect of which the council is a data controller, will be communicated by the council to data subjects by means of the council's overarching privacy notice and also service specific privacy notices. These are located on the council's website.

https://www.wyre.gov.uk/service-area-privacy-notices/privacy-notice?documentId=108&categoryId=20133

4.3 The council is committed to ensuring compliance with data processing legislation and will:

- respect the rights of each individual;
- be open and honest about the data it holds;
- provide training and support to officers responsible for the handling of personal data in the course of their duties;
- notify the ICO annually, that it processes data. This is a statutory requirement and notification must be kept up to date with any changes to the use of personal data being updated within 28 days (the council has two registration numbers Z5682712 (General processing) and ZA319367 (Electoral Registration) and;
- inform the ICO and in some instances the data subject of any data breaches.

5.0 Data Classification Scheme (DCS)

5.1 An important element of records management is classification. ISO 15489 defines classification as the "systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system".

5.2 The council's DCS features three classification categories; unclassified, protected and restricted. The DCS sets out the criteria and controls required when handling and processing council data.

6.0 Information Asset Registers (IAR)

6.1 Each service area within the council should have in place an up-to-date 'live' IAR. The register should set out the details of the information asset, its classification (as per the DCS), the council's legal basis for processing (if personal/sensitive data), the format it is held in (electronic or paper), the named Information Asset Owner (IAO), it's location and its retention period. There is a standard template for IAR's held on the HUB.

6.2 IAR's are subject to regular review by Internal Audit and spot checks may be carried out by the Data Protection Officer (DPO). However, it is the responsibility of the Head of Service (HOS) and/or Service Manager and any nominated IAO's to ensure that the register is reviewed regularly and kept up-to-date.

7.0 Roles and responsibilities

7.1 Senior Information Risk Owner (SIRO)
The Chief Executive serves corporately as the council's named SIRO in relation to information governance and data security related matters. The SIRO forms part of the council's Corporate Management Team (CMT) and therefore has a firm understanding of the strategic business goals of the council. They also understand how these goals may be impacted by information risks and how those risks may be managed. The SIRO's duties include; taking ownership of the organisation's risks registers, acting as a champion for information risk at CMT and directing the work of the council's DPO.

7.2 Data Protection Officer (DPO)
The DPO's minimum tasks, as defined by legislation are:

- to inform and advise the council and its employees about their obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities;
- advise on data protection impact assessments;
- train staff and conduct internal audits; and
- to be the first point of contact for supervisory authorities (ICO, Local Government Ombudsman) and for individuals whose data is processed (residents, employees, customers etc.).

7.3 Heads of Service (HOS) / Managers
HOS/Managers are ultimately responsible for the management of the records within their services, in accordance with this policy and for ensuing that their staff are aware of any data sharing protocols and storage and retention periods documented in the council's IAR's. HOS/Managers will be asked to make an annual declaration to the DPO to confirm that their services IAR have been reviewed and updated and that checks have been made to ensure the necessary technical measures are in place to protect the council's assets.

7.4 Information Asset Owners (IAO)

All council employees are responsible for creating and maintaining records in relation to their work that are authentic, up-to-date and reliable. However, service areas may also have individual nominated IAO for a specific system or a collection of records. IAO's ultimately have the necessary knowledge and skills to ensure that the asset is managed correctly and if not, to take the necessary action if any deficiencies in the relevant processes are identified. The IAO's core responsibilities are as follows:

- to ensure the capture of records is accurate and provides evidence of the service's activities;
- to make every effort to provide reliable data and records management;
- to observe and support any corporate polices and procedures;
- to understand any risks associated with processing and be pro-active about mitigation;
- to ensure that any contractors or third parties with access to council records are managing them in accordance with council policy and contracts/service level agreements, and;
- to provide the DPO with an annual declaration to confirm compliance with the terms of any written contracts or data sharing agreements and that the necessary technical measures are in place to protect the data being processed.

7.5 Information Governance Group (IGG)

The council has an IGG that meets formally approximately every 2 months. The membership is made up of the council's DPO and Deputy, ICT Service Manager, Legal Services Manager and Legal Executive. Other council officers are invited on an ad hoc basis depending on the agenda items. The group has an agreed terms of reference, which is reviewed annually. The group is responsible for the annual review of the council's information governance policies and procedures, prior to formal approval by the Audit Committee. All meetings have an agenda and are minuted by means of an action plan which documented any agreed actions. The action plan(s) is/are submitted to the SIRO through CMT on a quarterly basis.

7.6 ICT Service Manager (ICTSM)

The ICTSM is responsible for ensuring that all council ICT systems are designed and maintained to meet the council's security, records management and data protection obligations, and to ensure that they are strategically and operationally fit for purpose. The ICTSM is responsible for updating the IGG regarding any issues concerning the security of the council's systems and the records within them.

8.0 General record creation and record keeping

8.1 Each service area must have in place adequate record keeping systems (paper or electronic) that document its activities and allow for quick and easy

retrieval of information. It must also take into account any legal / regulatory requirements specific to the area of work. Systems should include:

- records arranged and indexed so they can be easily retrieved by any officer at any time;
- clear and documented procedures are in place for keeping the system updated;
- procedures and guidelines for referencing, indexing and version control;
- the ability to cross reference electronic and paper records; and
- documented procedural notes on how to use the system.

8.2 Details of these records should be documented in the individual services IAR which should be treated as a 'live' document, ensuring that when the data being held changes or moves, the IAR is updated to reflect this.

9.0 General record maintenance and security

9.1 Any record keeping system must be maintained so that the records are properly stored and protected and can easily be located and retrieved. This will include:

- ensuring that adequate storage accommodation is provided for records and they are kept clean and dry;
- monitoring the movement and location of records so that they can be easily retrieved and provide an audit trail;
- controlling access to the information, ensuring that all staff with access are aware of the arrangements for allowing access to certain types of information;
- identifying vital records and applying the appropriate protection and back-ups, which should be documented in individual business continuity plans; and
- ensuring non-current records, which are to be retained in accordance with individual IAR's are transferred in a controlled manner to a safe, secure archive facility, rather than being stored in offices.

10.0 Record retention and disposal

10.1 With increasing public access to our records, it is important that disposal of records happens as part of the managed process and is adequately documented.

10.2 HOS/Managers must have in place clearly defined arrangements for the selection of records for disposal, and for recording this work. The system should ensure that:

- records are reviewed and disposed of/transferred to an appropriate archive facility in accordance with the services

individual IAR and any other published regulatory or statutory retention requirement;

- records subject to FOI/EIR and Subject Access Requests (SAR) are not destroyed. It should be noted that it is an offence to alter or destroy records with the intention of preventing disclosure;
- an intended disposal/review date must be captured when creating electronic records. Furthermore, care must be taken when procuring an electronic system to ensure the system has the necessary capabilities to allow for on-going retention processes; and
- documentation of the disposal/transfer of records is completed and retained.

11.0 Emails

11.1 Emails are stored in Microsoft's UK facility that incorporates multiple levels of redundancy. This allows users to delete emails to their recycle bin, which are then recoverable for 14 days. There is a second stage recovery area, which allows recovery of emails for a further 30 days by a system administrator.

11.2 Any emails permanently deleted by users are recoverable up to the point at which the council implemented their current backup solution (May 2021). The system is configured to back up a maximum of 7 years of data and will then continue to back up on a rolling basis, aging and deleting data beyond this retention period.

11.3 An email warning is issued to users if they are reaching capacity in their mailbox. Users are encouraged to regularly housekeep their mailboxes so that they do not reach capacity limit. Managing emails with attachments, creating a filing system and refraining from leaving items in their inbox, sent items or deleted folders are suggested methods for good housekeeping techniques.

12.0 Corporate CXM system

12.1 There are many different systems across the organisation supporting the council’s activities. These are all, by definition, records management systems. In addition, the council is continuing to move forward with a corporate CXM system that either complements other council systems, serves to migrate unstructured data alongside these systems, or in some cases actually replaces these systems. The CXM administrator provides an annual declaration to the DPO to confirm they are satisfied that there are sufficient technical measures in place to protect the information held within the system.

13.0 Storing records offsite / hybrid working

13.1 All records that are taken and held offsite should be managed in accordance with this Policy, the council’s Data Protection Policy, the DCS and individual service IAR.

14.0 Contract clauses

14.1 The council's Legal Services Team in conjunction with the appropriate HOS/Manager and DPO will strive to ensure that any contracts with third party data processors have appropriate data protection, UK GDPR and record management clauses regarding the agreed and approved methods of information handling and storage and, if relevant, set out how information will be transferred back to the council at the end of a contract.

15.0 Training and awareness

15.1 Since all council employees will at some point be involved in creating, maintaining and using records, it is vital that everyone understands their responsibilities in relation to data security and their record management responsibilities that are set out in this policy.

15.2 Managers need to ensure that staff responsible for processing and managing records are appropriately trained / experienced and that all staff understand the need for record management.

15.3 The council will run training courses to ensure that all staff are aware of their obligations regarding data protection, FOI, EIR, SAR and general records management. These courses are considered mandatory and HOS/Managers should allow and support their staff in attending and completing the necessary training and awareness sessions being provided.

16.0 Reviewing the policy

16.1 This policy will be maintained and reviewed annually by the IGG and CMT (which includes the SIRO) before being formally approved by the council's Audit Committee.

This page is intentionally left blank

SUBJECT ACCESS REQUEST PROCEDURE

Document Control Information

Users of this document are responsible for familiarising themselves with the latest version on a regular basis. You should be aware that a physical copy might not be the latest available version. The latest version, which supersedes all previous versions, can be found on the council's hub.

Document Ref:	TYPE	**Version:**	1.0
Classification:	OFFICIAL	**Status:**	Draft
Effective from:	November 2022	**Review Date:**	November 2023
Prepared by:	Information Governance Manager	**Date:**	March 2022
Approved by:	Information Governance Group	**Date:**	March 2022
Change Forecast:	Annually, when there is a change in legislation or within the organisation		

Change History

Version	Date	Summary of Changes
1.0	01 April 2022	Procedures fully documented and submitted to CMT for approval
	27 April 2022	Approved by CMT
	07 November 2022	Submitted to Audit Committee for approval
		Approved by Audit Committee

CONTENTS

1. INTRODUCTION

1.1. Under the Data Protection Act (Act) 2018, an individual has the right to access personal information held about them by any organisation. This is known as the data subjects' right of access.

1.2. Wyre Council will ensure that individuals have access to their personal information, and are provided with a copy (where appropriate), within the required timescales legislated by the Act and the ICO.

1.3. To process a request, the data subject (or approved representatives) will normally need to send acceptable photo identification (e.g. copy of a Photo Driving Licence or Passport), proof of address (e.g. Bank Statement, Council Tax Bill, or Utility Bill) and any other supporting information required in relation to their request. The council are not able to charge a fee, in most cases. However legislation allows in certain circumstances to charge a fee if a request is deemed excessive or for duplicate request(s). If a fee is to be charged, the requester will be informed at the earliest opportunity and their permission will be sought to continue with the request given the fee required.

2. PURPOSE

2.1 To provide people receiving a service and/or their representatives with access to their personal records, in accordance with the Act.

2.2 To ensure council staff have a consistent approach when dealing with requests for personal information.

3. SCOPE

3.1 This procedure outlines how Wyre Council and its staff will provide access to personal records, compliant with the Act.

3.2 This procedure applies to living individuals and/or their representatives, wishing to access personal records. Access to records of individuals who are deceased will be dealt initially under the Freedom of Information Act 2000. Depending on the information or record being requested, if the record contains personal information this should be dealt with in the same way as those of individuals who are living. Access to a deceased person's data can be via the Access to Health Records Act (1990) or personal representative (executor or administrator of deceased person's estate or someone who has a claim resulting from the death. However, information can remain confidential even after death.

3.3 This procedure applies to all information, regardless of when it was created, in line with the retention periods documented within the council's Information Asset Registers.

4. LEGAL CONTEXT

4.1 The following legislation applies to this protocol:-

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Human Rights Act 2004
- Mental Capacity Act 2005

4.2 Related council documents:-

- Subject Access Request Form (Appendix A)
- Subject Access Request Online Form
- Subject Access Request (SAR) - Process flow chart (Appendix B)

5. RIGHTS OF ACCESS

5.1 Under the terms of the Act, every living individual has the right of access to personal information held about them unless an exemption applies. This applies to open and closed files. There are two notions of assistance whether information is personal data: whether it is significantly biographical, and whether it has the data subject as its focus, rather than some other transaction or event in which the data subject may have figured.

5.2 Whilst the council's preferred method for receiving an SAR is via the council's on-line form (see Appendix A), applications do not have to be in writing and can be received in different ways, such as email or verbally. Standard forms can make it easier for the council to recognise a subject access request and make it easier for the individual to include all the details that might be required to locate the information they are requesting. The form can be located using the following link https://www.wyre.gov.uk/site-search/results/?q=subject+access. Any member of staff could receive a request for access to records under the Act and employees can advise individuals how they can access their information by directing them to the on-line form. However employees **must not** make any attempt to respond to a subject access request and all requests should be forwarded to the Council's Information Governance Manager (IGM); Joanne Porter.

5.3 In the majority of cases, the council can no longer charge a fee for the processing of a data request. However, there are certain circumstances in which a fee can be charged. For example, if a request is deemed excessive or if a number of duplicate requests have already been received. This should be assessed by the individual service or team once a search for the relevant information or records has been completed, and if we hold what is required. If a fee is to be charged, the requester will be notified immediately. No information or records will be released until the fee has been received.

5.4 In most cases, the data subject will be required to provide a copy of photo identification and proof of current address which will need to be provided with their SAR application. However, if the requester is known to the council, ID may not always be required. In some instances, the requester may be asked a question that only they will know the answer to in order to validate their identity The decision on what ID is deemed appropriate is made by the IGM. Any requests for information or records made by a current council employee will not require them to provide the relevant ID. However the requests must all still be logged and processed in the usual way.

5.5 If a request for a council member of staff's employee records is received, then this should be forwarded to the IMG and processed in the usual way.

5.6 A representative (e.g. a parent, carer, solicitor or advocate) can apply for access to records on behalf of the data subject. The representative must provide consent from the data subject (if applicable). They may also need to provide a copy of their photo identification, proof of current address and further evidence of their right to access the records.

5.7 The month timescale will begin the day after receipt of a request and only when all the necessary ID checks have been made. Where a disproportionate effort would be needed to provide a copy of the records required, the requestor may be asked to provide further details to identify the specific information being requested. In both of these circumstances the month timescale will be suspended until this has been provided by them.

5.8 Under data protection legislation, there are certain circumstances where the one month timescale can be extended for up to a further two months. An extension may be applied if the

request is complex or we have received a number of requests from the individual. The requester will be notified within the first month if an extension is to be applied and the reasons why. If a Service feels they may wish to exercise this extension they must inform the IGM as soon as possible and must not wait until the first timescale has expired. In the limited situation where a fee can be charged for processing a request for right of access, a suspension will only be lifted once the payment has been provided by the applicant.

5.9 Where it is thought that a disproportionate effort is needed to provide a copy of the records required, the requestor may be asked to provide further details to identify the specific information being requested. On occasion, it may be necessary to allow access to a record (if possible) without providing a permanent copy of the record. This may not be possible where third party information is present.

5.10 Where the record contains information about another individual, consent to release the information may be required from that individual (known as the third party). However, in most cases this will just be redacted.

5.11 Where a record contains information supplied by another organisation, the decision to release this data lies with each individual organisation. If the decision is not to release, then the requestor will be directed to apply to the relevant organisation to gain access to the required information.

5.12 On receipt of the information, the data subject has the right to have any inaccuracies or in-factual information corrected, or to have comments or views added to the record. If the council refuses to act on this request, the individual may apply to the council to appeal this decision in the first instance. If they are still unhappy with the decision they may appeal to the Information Commissioner's Office (www.ico.gov.uk).

6. INFORMATION GOVERNANCE MANAGER'S (IGM) ROLE AND RESPONSIBILITIES

6.1 Applications to access information will be completed within the month timescale. The IGM is responsible for providing reminders to Heads of Service in respect of approaching deadlines. Performance indicators (numbers received to numbers outstanding and past deadlines) are reported to the Corporate Management Team on a quarterly basis.

6.2 Where there are large volumes of records, the IGM will liaise on a regular basis with the requestor to discuss any timescales and methods of delivery (electronic, hard copies or both). If the requester has not specified their preferred method, the requested data will be sent via encrypted email.

6.3 The IGM is responsible for identifying the appropriate service / manager who will coordinate the task of locating all of the appropriate records to obtain these for processing. This is normally the Head of Service or Service Manager.

6.4 The IGM will maintain a detailed log of all requests for information. This will include details of date received, details of any action taken, discussions which have taken place with the requester or the relevant service, and decisions which have been made regarding the processing of the request along with information in respect of compliance to the processing timescales.

6.5 Documentation relating to the applications will be retained in compliance with the relevant retention schedules. This will include the SAR logs, all correspondence and an archive copy of the information provided to the applicant.

7. REQUESTS MADE BY AN AGENT

7.1 Where a person with the capacity to make his/her own decisions has appointed an agent, such as a solicitor, the agent can make the request to access personal records. The request must be treated as if it had been made by the data subject.

7.2 The following information must accompany the request:

- A letter on company headed paper, which states the agent is acting on behalf of the data subject.

- Written consent for the agent to access information on the data subject's behalf. This must be signed by the data subject with the date of signature being within the last 3 months.

7.3 Each request will be considered in its own rights with the best interests of the data subject being considered in every instance (see section 11).

8. REQUESTS FROM OTHER ORGANISATIONS INCLUDING CHILDERN

8.1 All such requests to disclose or share information must be referred to the IGM. Information may be required in connection with safeguarding vulnerable individuals or the prevention and detection of crime and each request will be carefully considered before any information is disclosed. Only SAR's received from children 12+ will be considered. However in each instance, the IGM will carry out an assessment on the maturity and ability of the child to make a valid request.

9. INFORMATION PROVIDED BY OTHER ORGANISATIONS

9.1 There may be information within the documentation we hold about individuals that is being requested, that has been supplied by other organisations. If this is the case, it is the Head of Service / Service Manager's responsibility to seek authorisation from this organisation prior to it being provided to the IGM for release to the applicant.

10. REQUESTS FROM THE COURTS

10.1 All requests received from the Courts, by means of a sealed court order, must be complied with. Information must be supplied within the specified timescale and where no timescale is specified the request should be responded to promptly and within the one month timescale.

11. REQUESTS FROM THE POLICE

11.1 All general requests for personal information received from the Police, should be sent to the IGM who will coordinate the response to such requests.

12. REQUESTS FROM CONSUMER PORTAL SITES

12.1 All requests received from consumer portal sites e.g. **Rightly.co.uk** should be referred to the IGM. The council is not expected to register or pay to access a request for information. If a response is received in this format the IGM will make contact with the requester to ask them to supply the information in another format. If no response is received within 14 days of the original request, the request will be cancelled.

13. REDACTION

13.1 The removal of certain information (e.g. third party references) may be required from the data subject's information or records. Further support on redaction can be provided by the IGM.

14. FURTHER INFORMATION AND CONTACT DETAILS

14.1 If you have any questions in relation to this procedure, please contact the council's Information Governance Manager or email the council's dedicated information governance email address. InformationGovernance@wyre.gov.uk

Wyre Council
Information Governance
Civic Centre, Breck Road
Poulton-le-Fylde. FY6 7PU

Tel: (01253) 891000
Email: informationgovernance@wyre.gov.uk

Case Ref

(Office use only)

SUBJECT ACCESS REQUEST FORM
Data Protection Act 2018

This form is to be used when an individual (The Data Subject) wishes to access personal data held by Wyre Council. There is currently no fee payable for this service. Please send the completed form and appropriate identification to the address at the end of the form (section 9).

1 **Applicant** (to be completed in all cases)

Please select one of the following:

I am the Data Subject. I am requesting access to my personal information. ☐

I am not the Data Subject. I am requesting information on behalf of the data subject. ☐

2 **The Data Subject** (to be completed in all cases)

Surname: Forename (s):

Title: Mr, Mrs, Ms or Other (please specify): Date of Birth:

Previous name (s):

Address:

Previous Address:

Telephone number: Email address:

Please use below to provide details of any specific information you require, together with any relevant dates:

3 **Representatives Information** (to be completed if you are applying as the data subjects representative)

Surname: Forename (s):

Title: Mr, Mrs, Ms or Other (please specify): Date of Birth:

Previous name (s):

Address:

Telephone number: Email address:

Please use below to state your relationship to the Data Subject:

Please use below to explain your entitlement to receive the Data Subject's personal data (for example, Data Subject's signed authority, Lasting Power of Attorney or Parental Responsibility):

What authorisation have you enclosed?

4 **Identification**

You must provide two forms of identification to confirm the identity of the Data Subject, one which confirms their identity and one which confirms their current address. Please send one document from each list below. **Please do not send original documents,** good quality photocopies are acceptable.

Note: if you are a representative applying on behalf of the Data Subject, you must also provide two forms of identification which confirm your identity and current address.

Acceptable proof of identify:

- Current Passport
- Birth certificate
- Unexpired photo card driving licence (full or provisional)

Acceptable proof of current address:

- Utility bill dated within the last 3 months
- Council Tax bill for current year
- Unexpired old style paper driving licence
- Bank statement dated within the last 3 months
- Benefits Agency/State Pension correspondence (on letter header paper) dated within the last 3 months

5 **Format** (to be completed in all cases)

Your file(s) will be sent to you via encrypted email unless you tell us otherwise.

If you do not have access to a computer or would prefer to receive a paper copy. ☐

Please provide an email address for sending encrypted emails:

_____

When the encrypted email is sent it will be followed by a further email containing the password to open the file(s).

Should you experience problems opening the file(s) and in order to assist you please provide an answer to the following security questions. These will be asked when assistance is provided.

What is your mother's maiden name?

_____

Which primary school did you attend?

_____

What is your favourite colour?

_____

6 **Data Subject's declaration**

Please select one of the following statements:

I confirm I am the Data Subject. I wish to receive a copy of my personal records. ☐

I confirm I am the Data Subject. I have read and understood section 3 *(Representatives Information)* of this form, and I give my consent for my representative to receive a copy of my personal records on my behalf. ☐

Signed: Date:

7 **WARNING – it is a criminal offence to obtain another person's information by deception**

I confirm I am the appointed representative of the Data Subject. I wish to receive a copy of the Data Subjects personal records.

I confirm I am the Data Subject. I wish to receive a copy of my personal records.

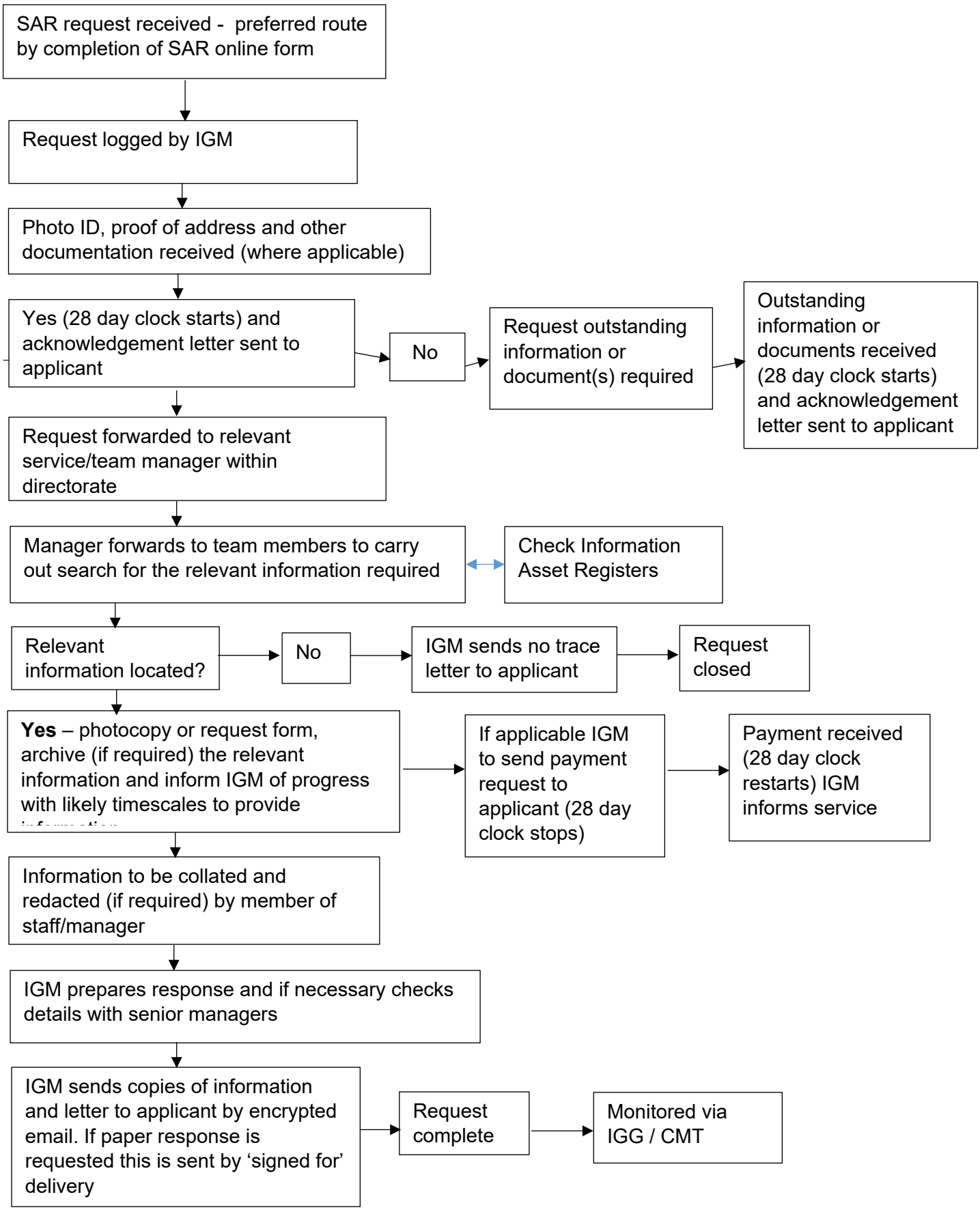
Signed: Date:

8 **Please send the completed form and appropriate identification and authorisation (if applicable) to the address below:**

Wyre Council
Information Governance Manager
Civic Centre
Breck Road
Poulton-le-Fylde
FY6 7PU

If you have any queries regarding this form please contact the Information Governance Manager on 01253 887503.

SUBJECT ACCESS REQUEST (SAR) – PROCESS FLOW CHART



Key

IGM – Information Governance Manager

IGG – Information Governance Group

CMT – Corporate Management Team

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	15 November 2022

ANNUAL REVIEW OF AUDIT COMMITTEE'S PERFORMANCE

1. Purpose of report

1.1 To consider CIPFA's Self-Assessment of Good Practice contained within the CIPFA publication 'Audit Committees - Practical Guidance for Local Authorities and Police 2018' and identify the actions necessary to ensure that the Audit Committee meets best practice guidance and provides value to the authority.

2. Outcomes

2.1 The determination of an improvement plan for the Audit Committee.

3. Recommendation

3.1 That the Audit Committee considers CIPFA's Self-Assessment of Good Practice at Appendix 1.

3.2 That the Audit Committee notes that a further review of their effectiveness will be completed after the May 2023 Elections to consider any new/updated CIPFA best practice guidance.

4. Background

4.1 Audit Committees are a key component of an authority's governance framework. Their function is to provide a high-level focus on assurance and the organisation's arrangements for governance, managing risk, maintaining an effective control environment, reporting on financial and non-financial performance and supporting standards and ethics.

4.2 An Audit Committee's effectiveness should be judged by the contribution it makes to, and the beneficial impact it has on, the authority's business.

4.3 Evidence of effectiveness will usually be characterised as 'influence', 'persuasion' and 'support'. A good standard of performance against recommended practice, together with a knowledgeable and experienced membership, are essential for delivering effectiveness.

4.4 Authorities are encouraged not to regard meeting the recommended practice as a tick box activity and are reminded that achieving recommended practice does not mean necessarily that the Audit Committee is effective. To help give a more rounded opinion of the Committee's effectiveness, further guidance is provided in CIPFA's Audit Committee publication in respect of a knowledge and skills framework.

5. Key Issues and proposals

5.1 The self-assessment at Appendix 1 has been completed by the Audit and Risk Manager (Chief Internal Auditor) and reviewed by the Corporate Director Resources (Section 151 Officer). At this stage, only one area has been identified where further improvement is considered beneficial. However, this may change at the meeting where the Audit Committee will be asked to contribute to a discussion with a view to ensuring the Audit Committee are still meeting the requirements of CIPFA's 'Self-Assessment of Good Practice'.

5.2 Since drafting this report and reviewing the self-assessment attached at Appendix 1, CIPFA have refreshed and re-issued their guidance for officers responsible for guiding audit committee's (Audit Committees: Practical Guidance for Local Authorities and Police; 2022 Edition), updated their Position Statement and have also issued new guidance aimed to assist members fulfil their roles and responsibilities. Therefore, an additional review of the Audit Committee's performance will be carried out following the May 2023 elections to ensure the new/updated guidance is taken into consideration.

Financial and legal implications	
Finance	There are no specific financial implications arising from this review of the effectiveness of the Audit Committee.
Legal	There are no specific legal implications arising from this review of the effectiveness of the Audit Committee.

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
Karen McLellan	01253 887586	karen.mclellan@wyre.gov.uk	02.11.22

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

List of appendices

Appendix 1 – CIPFA Self-Assessment of Good Practice

CIPFA Self-Assessment of Good Practice – November 2022

Good practice questions		Yes	Partly	No	Comments
Audit Committee purpose and governance					
1	Does the authority have a dedicated Audit Committee?	✓			The Audit Committee has been in place since December 2005.
2	Does the Audit Committee report directly to Full Council?	✓			A periodic report is submitted to Full Council with the last report being considered on 14 April 2022.
3	Do the terms of reference clearly set out the purpose of the committee in accordance with CIPFA's Position Statement?	✓			The terms of reference were last reviewed in March 2022 to ensure they accurately reflected CIPFA's guidance 'Audit Committee's – Practical Guidance for Local Authorities and Police 2018'.
4	Is the role and purpose of the Audit Committee understood and accepted across the authority?	✓			
5	Does the Audit Committee provide support to the authority in meeting the requirements of good governance?	✓			The Audit Committee provide assurance on the adequacy of internal control, risk management, the integrity of financial reporting and the annual governance processes. They also oversee responsibility for the council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the approval of policies in relation to Cyber Security and compliance to the UK's General Data Protection Regulations

Good practice questions		Yes	Partly	No	Comments
					2018.
6	Are the arrangements to hold the Audit Committee to account for its performance operating satisfactorily?	✓			
Functions of the Committee					
7	Do the Audit Committee's terms of reference explicitly address all the core areas identified in CIPFA'S Position Statement?	✓			The Audit Committee's terms of reference are in accordance with CIPFA's 'Audit Committees - Practical Guidance for Local Authorities and Police 2018'.
	▪ good governance ▪ assurance framework ▪ internal audit ▪ external audit ▪ financial reporting ▪ risk management ▪ value for money or best value ▪ counter-fraud and corruption ▪ supporting the ethical framework				
8	Is an annual evaluation undertaken to assess whether the committee is fulfilling its terms of reference and that adequate consideration has been given to all core areas?	✓			Although the annual evaluation is completed by the Audit and Risk Manager (Chief Internal Auditor) and reviewed by the Corporate Director Resources (Section 151 Officer), the annual review of effectiveness gives the Audit Committee the opportunity to assess if it is fulfilling the terms of reference.
9	Has the Audit Committee considered the wider areas identified in CIPFA's Position Statement and whether it would be appropriate for the committee to undertake them?	✓			The Audit Committee already participate by considering governance and risk. The Code of Practice on Treasury Management requires a body to be nominated and responsible for ensuring effective scrutiny of the Treasury Management Strategy and policies. The Council has nominated the Overview and

Good practice questions		Yes	Partly	No	Comments
					Scrutiny Committee (Cabinet 25/03/2015).
10	Where coverage of core areas has been found to be limited, are plans in place to address this?	N/A	N/A	N/A	There have been no instances where coverage of core areas has been found to be limited.
11	Has the Audit Committee maintained its non-advisory role by not taking on any decision-making powers that are not in line with its core purpose?	✓			The Audit Committee does not take on any decision making powers that are not documented within its terms of reference.
Membership and support					
12	Has an effective Audit Committee structure and composition of the Committee been selected? This should include: ▪ separation from the executive ▪ an appropriate mix of knowledge and skills among the membership ▪ a size of committee that is not unwieldy ▪ consideration has been given to the inclusion of at least one independent member (where is it not already a mandatory requirement).	✓ ✓	✓	✓	Whilst individual Members of the Audit Committee (AC) may also serve on Overview and Scrutiny the Audit Committee is independent of the scrutiny function. The Audit Committee Chairman is not a member of the Executive. **Action: Whilst the size of the Audit Committee is currently large at 14, a review of the membership is recommended to take place in 2023, with a view to reducing the overall number but including an independent member/s as recommended in CIPFA's revised position statement 2022.**
13	Have independent members appointed to the committee been recruited in an open and transparent way and approved by the Full Council.			✓	The Audit Committee membership does not contain any independent members but this will be kept under review.

Good practice questions		Yes	Partly	No	Comments
14	Does the Chairman of the Audit Committee have appropriate knowledge and skills?	✓			The Audit Committee Chairman was appointed in May 2015. She holds an Associate Chartered Accountants qualification (ACA) and has previously worked in managerial roles within the audit environment.
15	Are arrangements in place to support the Audit Committee with briefings and training?	✓			Training is provided to the Audit Committee in accordance with their Audit Committee Work Programme. In addition, the Committee members will receive briefings as part of the Audit Committee agenda as and when required.
16	Has the membership of the Audit Committee been assessed against the core knowledge and skills framework and found to be satisfactory?	✓			The induction training in May 2019 covered the core areas of the knowledge and skills framework. Any new Members are trained as and when appointed to the Committee. On-going regular attendance will ensure members complete the work programme thereby continually enhancing their knowledge and skills.
17	Does the Audit Committee have good working relations with key people and organisations, including external audit, internal audit and the Chief Financial Officer?	✓			The Corporate Director Resources (Section 151 Officer), Head of Governance and Business Support and the Audit and Risk Manager (Chief Internal Auditor) routinely attend every Audit Committee meeting, with the exception of the meeting to approve the Statement of Accounts, which the Head of Governance and

Good practice questions		Yes	Partly	No	Comments
					Business Support and the Audit and Risk Manager does not attend. A representative from the council's External Auditors is frequently in attendance.
18	Is adequate secretariat and administrative support to the Audit Committee provided?	✓			Each meeting is attended by an officer from the Council's Democratic Services Team. The meetings are minuted and published on the Council's Internet.
Effectiveness of the Committee					
19	Has the Audit Committee obtained feedback on its performance from those interacting with the committee or relying on its work?	✓			Feedback is sought annually from the External Auditor.
20	Are meetings effective with a good level of discussion and engagement from all members?	✓			Members routinely ask questions at Audit Committee and have written to the Executive where they want a further explanation and updates following audit reports.
21	Does the Audit Committee engage with a wide range of leaders and managers, including discussion of audit findings, risks and action plans with the responsible officers?		✓		Following the receipt of a final audit report, the Audit Committee have the opportunity to call in Service Managers to challenge them on audit findings, outstanding actions or any associated risks.
22	Does the Audit Committee make recommendations for the improvement of governance, risk and control and are these acted on?	✓			If areas of work receive a 'limited or minimal/no overall assurance opinion', the Audit Committee may make recommendations for further audit reviews, more frequent updates and may also request the intervention of the

Good practice questions		Yes	Partly	No	Comments
					relevant Director or Portfolio Holder for additional assurances that the weaknesses are being addressed.
23	Has the Audit Committee evaluated whether and how it is adding value to the organisation?	✓			During their induction in May 2019, Audit Committee Members were asked to give examples of where they felt the AC added value and if there was anything else the committee could be doing to improve the value added to the organisation.
24	Does the Audit Committee have an action plan to improve any areas of weakness?	N/A	N/A	N/A	No areas have been identified following this review.
25	Does the Audit Committee publish an annual report to account for its performance and explain its work?	✓			A periodic report is submitted to Full Council with the last report being considered on 14 April 2022. The report explains the work of the Committee and more specifically details the reports that been submitted to the Audit Committee during the year.

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