Audit Committee Agenda

Wyre Borough Council
Date of Publication: 18 November 2020
Please ask for: Emma Keany
Democratic Services Officer
Tel: 01253 887476

Audit Committee meeting on Thursday, 26 November 2020 at 6.00 pm in the Council Chamber - Civic Centre and via WebEx.

Members of the public will be able to view the meeting via the Council's YouTube page (https://www.youtube.com/WyreCouncil).

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 - 6)

   To confirm as a correct record the minutes of the last meeting of the Audit Committee held on 10 March 2020.

4. **Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)** (Pages 7 - 10)

   Report of the Legal Services Manager.

5. **Internal Audit and Risk Management- Progress Report** (Pages 11 - 32)

   Report of the Corporate Director Resources (Section 151 Officer)

6. **Annual Review of Financial Regulations and Financial Procedure Rules** (Pages 33 - 36)

   Report of the Corporate Director Resources (Section 151 Officer)

7. **Annual Review of the Council's Counter Fraud Policies** (Pages 37 - 40)

   Report of the Corporate Director Resources (Section 151 Officer)

8. Approval of the Council's Data Protection Policy and Procedures (Pages 41 - 60)

Report of the Head of Governance (Data Protection Officer)

9. Annual Review of the Audit Committee's Performance (Pages 61 - 70)

Report of the Corporate Director Resources (Section 151 Officer)

10. Statement of Accounts (Post Audit) 2019/20

Report of the Corporate Director Resources (Section 151 Officer)

(Papers to follow)

11. Management Representation Letter 2019/20

Letter to be signed by the Chairman of the Audit Committee and the Corporate Director Resources (Section 151 Officer) on 26 November 2020.

(Papers to follow)

12. Report of Those Charges with Governance (ISA 260) 2019/20

Report of the Corporate Director Resources (Section 151 Officer)

(Papers to follow)

Audit Committee Minutes

The minutes of the Audit Committee meeting of Wyre Borough Council held on Tuesday 10 March 2020 at the Council Chamber, Civic Centre, Poulton-le-Fylde.

Audit Committee members present:
Councillors McKay, Ingham, R Amos, E Ellison, Longton, Minto, O'Neill, Stirzaker, L Walmsley, Fairbanks and Webster.

Apologies for absence:
Councillors Cartridge, Holden and Moon.

Other councillors present:
Councillor I Amos.

Officers present:
Emma Keany, Democratic Services Officer
Joanne Billington, Head of Governance
Clare James, Corporate Director Resources and Section 151 Officer
Paul Hewitson, External Auditor (Deloitte LLP)

No members of the public or press attended the meeting.

---

36 Declarations of interest

None.

37 Confirmation of minutes

Agreed that the minutes of the Audit Committee meeting held on 19 November 2019 be confirmed as a correct record.

38 Review of Audit Committee's Terms of Reference

The Corporate Director Resources (Section 151 Officer) submitted a report that reviewed the Audit Committee's Terms of Reference.

The Head of Governance discussed the report and highlighted a change that the External Auditors, Deloitte, had requested be added to the committee's terms of reference. The change was to ensure that the committee annually reviewed the impartiality of the external auditors so that could ensure that they remained objective in their audit work without this being impaired by

additional work provided to the council.

Joanne Billington asked the external auditor, Paul Hewitson, how he would envision the review would take place. He responded by stating it may be ideal to review the work of the external auditors after the ISA 260 (Report to those charged with Governance) had been considered by the committee. He also suggested that the committee should review their impartiality every time Deloitte LLP was chosen to deliver other work. Mr Hewitson also discussed how the review could be delegated to officers but this would need to be documented.

Agreed:

1. That the following additional bullet point be inserted under the section on External Audit in the proposed terms of reference:
   - To consider periodically (at least annually), whether the auditors appointed to carry out the external audit function remain independent and objective and, that their judgement in carrying out that role has not been impaired as a consequence of their participation in any non-audit reviews, service or advice provided to the Council.

2. That, subject to the inclusion of the addition in 1 above, the revised terms of reference attached as Appendix 1 of the report accurately reflected the role of the Committee.

3. That the full Council be recommended to approve the revised terms of reference and to include them as Article 7 in Part 2 of the Constitution, in place of the previous version.

39 Internal Audit Strategy and Audit Plan 2020/21

The Corporate Director Resources (Section 151 Officer) submitted a report that reviewed the Internal Audit Strategy and annual Audit Plan for the 2020/21 financial year.

The Head of Governance highlighted key aspects of the report. She discussed the audit team structure, the fact that the plan had not identified any need for Lancashire County Council auditors to cover any work due to the comprehensive assurance mapping that is now completed, the shared audit service with Lancaster City Council and the reference, in Appendix 2, to Marine Hall.

Agreed:

1. That the Internal Audit Strategy, attached as Appendix 1 of the report, and the Annual Audit Plan for 2020/21, attached as Appendix 2 of the report, be approved.

40 Internal Audit Charter

The Corporate Director Resources (Section 151 Officer) submitted a report regarding the annual review of the internal audit charter.

The Head of Governance provided an overview to the report and the purpose of the charter and informed the committee that there had been no changes to this document since its last review in 2019.

Agreed:

1. That the Internal Audit Charter and Code of Ethics attached at Appendices 1 and 2 be approved.

41 Letter from the Public Sector Audit Appointments Limited (PSAA)

The Corporate Director Resources (Section 151 Officer) provided a verbal update regarding the letter from the Public Sector Audit Appointments Limited (PSAA).

The committee noted the letter.

42 External Audit Plan 2019/20

Paul Hewittson, External Auditor (Deloitte LLP), submitted a report setting out how Deloitte would carry out their audit work on Wyre's activities and performance for the year ending 31 March 2020. He drew attention, in particular, to the following key elements of the plan:

- Where the most risk had been identified and would subsequently mean the work that the external auditors would dedicate most of their time towards;
- How 'materiality' would be determined (on page 49 of the printed agenda);
- The 'significant risks dashboard' (on page 51-54 of the printed agenda);
- The responses on insights raised in the previous audit (on page 55 the printed agenda) and
- Arrangements for the confirmation of the independence of the audit team and fees (on page 60 of the printed agenda).

Members of the Committee initially expressed some concern about the use of a 'materiality' figure of £1.2 million (based 2% of the Council's gross income), leading to miss-statements of less than £61,000 not routinely being reported to the Committee. However, they were satisfied by the External Auditor's explanation that on the basis he had described, £61,000, represented approximately 5% of 2% of the Council's Total Gross Income and was therefore a reasonable reporting threshold to use. All errors below the £61,000 threshold are reported to the s.151 officer and their deputy.

Members of the Committee also indicated that they were comfortable with the independence of the audit team, even with the additional work carried out.

The committee noted The External Audit Plan for the year ending 31 March 2020.

43 Periodic private discussion with the Chief Internal Auditor

Following the conclusion of the formal meeting, members of the Committee were given the opportunity to have their private periodic discussion with the Head of Governance, as provided for in the Committee's work programme.

(The Head of Finance, the Democratic Services Officer and the External Auditor left the room for this item).

44 Time and date of next meeting

Tuesday 5 May 2020 at 6pm.

The meeting started at 6.00 pm and finished at 6.51 pm.

Date of Publication: 29 May 2020

Report of:	Meeting	Date	Item no.
Mary Grimshaw, Legal Services Manager	Audit Committee	26 November 2020	4

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

1. Purpose of report

1.1 To review the authority's use of RIPA since it was last considered at the Audit Committee in November 2019.

2. Outcomes

2.1 Evidence that the council complies with current legislation.

3. Recommendations

3.1 Members are requested to note that there have been no authorisations granted for directed surveillance or covert human intelligence source under the Regulation of Investigatory Powers Act 2000 since 2012.

3.2. Members are requested to note that there are no changes to the RIPA policy which was last updated and approved by the Audit Committee in November 2019. The RIPA policy can be found at the following location. https://wyregovuk.sharepoint.com/sites/LegalDepartment/SitePages/Regulation-of-Investigatory-Powers-Act.aspx

4. Background

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

4.2 From 1 November 2012, the Protection of Freedoms Act 2012, became effective. It introduced a more restrictive approach to the use of RIPA by local authorities by limiting the use of direct authorisations to serious crimes, i.e. those crimes punishable by a maximum custodial sentence of six months or more or those constituting an offence of selling alcohol or tobacco to children. The application must also have judicial approval by a magistrate before an authorisation takes effect and the magistrate needs to be satisfied that there are reasonable grounds for believing that the requirements of RIPA are met.

5. Key Issues and proposals

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

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

- An annual review of the policy ensuring that it remains fit for purpose.

5.2 There is a requirement for the council to nominate a Senior Responsible Officer, who will be responsible for:

- The integrity of the RIPA process in place within the council to authorise surveillance and the covert use of human intelligence source (CHIS);

- Compliance with the legislation and codes of practice;

- Engagement with the Commissioners and inspectors when they conduct their inspections; and

- Overseeing the implementation of any post inspection action plan recommended by the Commissioner.

5.3 There is also a requirement to have a Senior Responsible Officer who oversees the competence of Authorising Officers and the processes in use in the authority. Both of these roles are allocated to the Legal Services Manager.

5.4 There has been no authorisations issued under RIPA since 2012.

5.5 The Investigatory Powers Commissioner's Office (IPCO) has taken over the inspection and oversight functions on RIPA, previously carried out by the Surveillance Commissioner's Office and the IPCO and his assistants have confirmed that they will continue to ensure RIPA compliance by

conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections when a local authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. However, a desktop inspection will always be followed by an onsite inspection.

5.6 The council's last inspection was carried out by a remote assessment in March 2019.

5.7 Following the desktop-based documentary inspection, the Inspector issued a report in April 2019, which concluded that the council's policy and guidance regime was clear and comprehensive and that regular refresher training carried out by the officers was appropriate. He drew the council's attention to the usefulness and accessibility of social media in assisting with the council's enforcement processes and the advice contained in the revised Home Office Covert Surveillance and Property Interference Code of Practice.

5.8 In light of the Inspector's report and following refresher training undertaken by officers where the use of social media was addressed, paragraph 11 of the Council's policy at Appendix A was updated, together with a few other minor changes. The amendments were approved by the Audit Committee on 19 November 2019. A new social media process was also added at Appendix 11 which outlines the process to be followed by officers when considering using social networking sites for enforcement purposes, in investigations or to gather evidence.

5.9 Following the Corprate Management Team restruvcutre in December 2019, the Corporate Direcotre Resouces requires training on RIPA and this will be arranged at the earliest opportunity following following the response phase of the Covid-19 pandemic.

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

Processing Personal Data

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

report author	telephone no.	email	date
Mary Grimshaw	01253 887214	Mary.grimshaw@wyre.gov.uk	25.10.2019

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	26 November 2020

INTERNAL AUDIT AND RISK MANAGEMENT - PROGRESS REPORT

1. Purpose of report

1.1 To review progress in relation to the 2020/21 Audit Plan, Risk Management and consider progress against the action plan resulting from the 2019/20 Annual Governance Statement.

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 Head

of Governance 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 2019/20 Annual Governance Statement are attached at Appendices 1, 2, and 3.

Financial and legal implications	
Finance	The annual programme of audits is performed by the in-house team. To date no audit days have been supplied by Lancashire Audit services. However the budget remains in place in case additional support is needed in quarter four of 2020/21.
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 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
Joanne Billington	01253 887372	Joanne.billington@wyre.gov.uk	18.11.2020

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 2019/20 - Action Plan update

Appendix 1

INTERNAL AUDIT PROGRESS REPORT – JUNE 2020 to NOVEMBER 2020

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. 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."***

Members of the Audit Committee should note that copies of both terms and reference and internal audit reports are published on the council's Intranet. Access to the supporting files is available to Members of the Audit Committee on request. The table overleaf summarises audit work performed since the last progress reported at the Audit Committee meeting on the 16 June 2020 held under emergency powers.

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 council also works closely with the Association of Local Authorities Risk Managers (ALARM) and our insurer, Zurich Municipal.

Whilst the council has an annual contract with Lancashire Audit Services (LAS) at a rate of £365 per day, no audit days have yet to be allocated for 2020/21. However regular consultation takes places to ensure we continue to benefit from their wealth of experience and extensive client base.

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.

Audit Work Performed June to November 2020

As summarised below the following reviews have been performed and reports issued since the last progress report was delivered in the Annual Audit report in June 2020.

Wyre Council Reports

AUDIT OPINION DEFINITIONS

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.

DEFINITION OF PRIORITY RANKINGS

Level 1	Non-compliance with Financial Regulations and Financial Procedures Rules, Employees Code of Conduct, staff instructions etc. which could have a material effect on the Council's finances or, a lack of or serious weakness in key control(s) which may impact on the Council's finances or operational performance.	Immediate Action Required
Level 2	Non-compliance with Financial Regulations and Financial Procedures Rules, Employees Code of Conduct, staff instructions etc. which have a minor effect on the Council's finances or operational performance.	Within 3 months
Level 3	A lack of, or weakness in an internal control which does not pose an immediate high level of risk, but if left unresolved could expose the Council to financial losses or reduce operational performance.	Within 6 months
Level 4	Suggestions for improvement of internal controls of a minor nature.	Within 9 months
Level 5	Suggestions for improvements, efficiencies in service delivery.	None

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
Audit work from 2019/20 completed since June 2020								
Inspection Regime – Site Inspections	**Final Report Issued October 2020**	**0**	**1**	**6**	**0**	**0**	**Fair**	Areas have been identified where improvements could be made to strengthen the control environment, namely; • A documented inspection policy / procedure or staff guidance manual has not been compiled for by all departments; • Formal training on the completion of inspections has not been given to all inspection staff; • Inspections are not carried out in accordance with the agreed frequency in all instances; • The recording of the actions taken to repair any defects identified is not completed and retained by all departments; • Accurate inspection records of the areas inspected and the defects identified are not completed in all instances; • Formal retention periods for completed inspection records have not been agreed for all departments; and • Monitoring of inspection processes and feedback to staff is not routinely undertaken.
Planning – Local Authority Education Contributions	**Final Report Issued October 2020**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**Excellent**	No areas were identified that required improvements to the control environment.
Grant Management	**Fieldwork in progress**							The overall objective of the audit is to review the controls in place to manage grant funding where the council have accountable body responsibilities 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. This work will focus on covid-19 business

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								grants.
Citizens Access Portal	**Position statement to be issued December 2020**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	N/A
Civica Pay	**Position statement to be issued December 2020**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	This piece of work will be delayed until February 2021 at the earliest.
2020/21 Audit work								
Building Maintenance (follow-up)	**Report currently being drafted**							The overall objective of the audit is to review the progress that has been made in implementing the actions following the audit that was originally completed in November 2019.
IR35 (follow-up)	**Fieldwork in progress**							The overall objective of the audit is to review the progress that has been made in implementing the actions following the audit that was originally completed in October 2018.
Community Lottery (follow-up)	**Fieldwork in progress**							The overall objective of the audit is to review the progress that has been made in implementing the actions following the audit that was originally completed in December 2019.
Beach Management Scheme	**On-going**							The Senior Auditor is attending regular beach management project meetings to provide advice and support in respect of internal control, risk management and the overall governance framework. It is not anticipated that a report will be published in relation to this work, however an overall opinion on

TITLE	STATUS	RECOMMENDATIONS – PRIORITY RANKINGS					AUDIT OPINION	Summary
		1	2	3	4	5		
								the control environment in relation to this project will be provided in the Internal Audit Annual report for 2020/21.
Performance Management	**Report currently being drafted**							The overall objective of the audit is to review the controls in place around the council's performance management systems and processes 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.

Outstanding Audit's to be completed in 2020/21 (ending 31 March 2021)

No internal audit work was completed during the period 1 April to 31 August 2020 owing to both the Head of Governance and the Senior Auditor being redeployed to work with the Community Hubs during the on-going pandemic. In addition, from the 2 November 2020, the Senior Auditor returned to supporting the Community Hubs restarted for the borough's Clinically Extremely Vulnerable residents.

The audit plan for 2020/21 that was approved in March 2020 is in the process of being revised to take into consideration the loss of audit days during quarter one and two and the reduced resources going forward given the on-going support being provided to the Community Hub. The revised audit plan will focus on areas of high risk and will also include assurance work around the processing of Covid related grants. Once agreed with the Corporate Director Resources, the revised plan will be circulated to the Audit Committee.

Other audit work undertaken during the year 2020/21

National Fraud Initiative – Cabinet Office data matching exercise

The Compliance Team have been finalising the investigation of the matches of the 2018/19 NFI exercise. A report will be submitted to the next Audit Committee (March 2020). In addition the 20/21 exercise is now underway. The Head of Governance is currently in the process of uploading a number of datasets in line with Cabinet Office requirements. The deadline for completion is December 2020 with the matches being released over the next few months. A discussion will take place with the Compliance Manager to identify a timelier follow-up process for the matches of the 20/21 exercise, recognising that some allowances may still need to be made depending on the pandemic situation.

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

The Council's Data Protection Officer (DPO) and Deputy DPO continue to work to ensure the Council is compliant with the Data Protection Act 2018 (the Act) and the enshrined General Data Protection Regulations (GDPR) which came into force in May 2018. The DPO reports quarterly to the Corporate Management Team, with the last update being on the 11 November 2020 and reported the following;

- The Elections and Information Governance Manager has now completed a review of the Council's compliance to the Transparency Code. Responsible officers have been emailed detailing the action needed to ensure compliance. A follow-up review will be completed in the new-year.

- Following the completion of a GDPR compliance audit at Lancaster City Council, Wyre will use the action plan produced to benchmark Wyre's compliance with GDPR. The intention was to complete the work in 2020/21, however, owing to Covid and limited resources, audit days will now be allocated for this work in the Audit Plan for 2021/22.

- Owing to Covid-19 and other work commitments, the Information Governance Group have not met since 29 January 2020. It has been agreed with the group

members that these meetings will now take place via TEAMS and will commence in the new-year.

- Work to identify a training module to be used at the Corporate Induction and as a re-refresh for all existing staff in relation to GDPR and Information Security is currently on-hold owing to the on-going Covid pandemic. There is a concern that the only induction new starters have in relation to these topics is the receipt of the Data Protection (DP) Policy and Breach Reporting Procedures in their indication pack. They are however asked to sign a declaration of understanding. The Data Protection Policy has been temporally updated to reflect this.

- The DPO will carry out a number of security sweeps of the Civic Centre in December to ensure staff are continuing to keep data safe and secure during these unprecedented times.

- The FOI / EIR training session and the pre-council GDPR training session that was scheduled to take place on the 14 May has been postponed until further notice. Discussions are taking place with the External Trainer as to how this training can be delivered remotely.

Anti-Fraud and Corruption

All the council's counter fraud policies are reviewed annually by the Audit Committee, with the last review being completed in November 2020. The policies are located on SharePoint 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 2020/21. The money laundering legislation was amended in January 2020. The policy will be updated to reflect the changes in legislation.

Gifts, Hospitality and Registering Interests – There have been only two declarations made by council officers receiving gifts and hospitality since the 1 April 2020.

Whistleblowing / Investigations - There have been no whistleblowing calls during 2020/21 that have required internal audit investigation.

RISK MANAGEMENT PROGRESS REPORT

Operational Risks

Progress on the embedding of risk management is reported to the Audit Committee via six monthly reports by the Head of Governance. 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.

Risk workshops are normally held in February each year with each service unit identifying any new risks that may occur during the year preventing the achievement of individual service plans. It is also an opportunity to review progress made in respect of any existing risks, remove risks that are no longer valid and action plan to mitigate against identified risks wherever possible. However, owing to the on-going pandemic, operational risk workshops have not taken place this year.

All staff who have responsibilities for identified risks have been encouraged to review their risks and update their action plans accordingly. However, to date, little response has been received. This has been raised at the Chief Internal Auditor's quarterly update to CMT and a reminder will be issued to staff responsible for operational risks, reminding them of the importance of risk management and the requirement to document the progress being made to mitigate the risks they have identified.

In addition, the Audit Committee are encouraged to go and view the risks identified by each service unit and challenge any areas were limited progress is being made to mitigate the risks identified.

It is anticipated that operational risk workshops will be arranged via TEAMS in January 2021 as normal following the strategic risk workshop.

https://wyregovuk.sharepoint.com/sites/Governance/SitePages/Risk-management.aspx

Strategic Risks

The Corporate Management Team (CMT) met on the 10 February 2020 to carry out the annual strategic workshop. The results of the workshop were presented to the Committee at its meeting in June 2020. Strategic risks and any subsequent actions are reviewed every quarter by CMT. Any changes to the ratings are documented and supported by a valid reason and sufficient evidence. The last quarterly update was carried out on the 14 October 2020. The results of this review will be reported verbally to the Audit Committee at its November meeting.

The next strategic risk workshop will be held in February 2021. The date has yet to be confirmed.

Brexit Risks

In preparedness for the UK leaving the European Union, the council has populated a BREXIT risks register which is reviewed on a regular basis following updates from Central Government, CMT and Head of Services. The last review was completed in November 2020. The BREXIT register can be found on SharePoint following this link

https://wyregovuk.sharepoint.com/sites/Governance/SitePages/Brexit.aspx

ICT Risks

In 2017, SOCITM carried out an independent review of the council's ICT Service. A number of high level recommendations were made to improve the delivery of the service, one being the identification and compilation of an ICT risk register. This was completed in January 2018 and is reviewed quarterly by the Service Director Performance and Innovation, Head of ICT and the Senior Auditor. The last review was completed on 21 September 2020 and a verbal update will be provided at the meeting.

2019/20 ANNUAL GOVERNANCE STATEMENT ACTION PLAN – POSITION AT NOVEMBER 2020

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
Information Governance	C/F 2018/19	The council continues to work towards ensuring full compliance with the changes to the Data Protection Act and the GDPR. Whilst significant work has been completed in respect of contracts, data subject rights and privacy, further work is still required in respect of data sharing and validation of the council's information asset registers.	A GDPR compliance audit was included in the 2019/20 audit plan and was to be completed by an external provider under the Lancashire County Council, ICT audit framework. Unfortunately, owing to the Covid-19 pandemic, this piece of work has been delayed and will be rolled to the 2021/22 audit plan. In the meantime, the Head of Governance will use the report issued for Lancaster City Council to benchmark Wyre's policies and procedures.	Jo Billington / Jo Porter On-going	Owing to the on-going pandemic and limited staffing, the Data Protection Officer has not been able to carry out a review of the council's compliance to GDPR using Lancaster City Council's action plan. A piece of work will be included in the 2021/22 audit plan. Any immediate or significant concerns will be reported to CMT and Audit Committee as part of the routine quarterly / six monthly reporting.
Ethical Governance	C/F 2018/19	The council has conducted an Ethical Governance Survey to ensure officers know and understand the council's key policies and procedures around expected behaviours. It is suggested that the survey also be rolled out to elected Members. The last survey of this nature was completed several years ago.	Owing to Covid-19 this has been delayed. Members will be asked to complete the survey later in the year.	Jo Billington Autumn 2020	A decision has been made to carry out this survey in 2021 as a number of other consultations and surveys have already been completed this year or are scheduled to be.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
Staffing Capacity	C/F 2018/19	The council has recently had difficulty recruiting and retaining staff to key roles throughout the organisation. Benchmarking at CMT level has been completed and this resulted in a restructure in late 2019. Discussion at the strategic Human Resources group identified that recruitment and retention of staff is proven to be an issue across Lancashire.	Roles to be benchmarked need to be identified and benchmarked with other Local Authorities,	Liesl Hadgraft On-going	Initial data received suggests it is not possible to make the necessary comparisons of jobs as structures were not comparable and as such roles were not the same. Owing to the on-going pandemic this has not been progressed any further.
ICT Disaster Recovery	C/F 2018/19	Whilst an ICT disaster recovery plan has recently been drafted, this has yet to be finalised. Formal start-up / shutdown process has been developed and a disaster recovery proposal is being progressed to provide a fully resilient solution. Discussions have taken place with a number of companies regarding different solutions and subsequent in depth reviews have been conducted. A portfolio holder report is being drafted which should be submitted for review in August, however work has been delayed due to	The Disaster Recovery Plan needs to be finalised and rolled out as soon as possible.	Steve Simpson ASAP	Owing to the on-going pandemic and the additional pressures this placed on ICT, this piece of work has been delayed. It is expected this work will be picked up early in the new year.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
		Windows 10 / server migration and owing to the COVID-19 pandemic.			
Staff Survey	2019/20	It was identified that a full staff survey had not been carried out for some time. Previously, the council has also carried out a number of staff 'engagement sessions' giving staff an opportunity to raise or voice concerns. There have been no sessions of this nature for over a year.	Once normal business activities resume, the council should consider carrying out a further staff survey and / or possibly carrying out further engagement sessions pending on future instructions regarding social distancing. During the Covid-19 pandemic the council completed a survey on home working.	Liesl Hadgraft / CMT December 2020	Owing to the on-going pandemic a staff survey has yet to be completed. HR are drafting a survey to be issued before Christmas, with a Health and Wellbeing focus.
Office 365/ Microsoft Teams	2019/20	The Council has started to move over to Windows 10 and in doing so is using Microsoft Office 365 and Teams. However it is understood that there are a number of training issues and staff are not using both systems to their full potential.	Guidance should be added to BRIAN and training should be rolled out to all officers to ensure staff can fully embrace the new technology.	Steve Simpson April 2020	During the pandemic, ICT uploaded a number of documents to SharePoint to assist officers with the move to the new technology. Staff are encouraged to log any requests for training through TOP DESK. **On-going**
Training and Development / GDPR Training	2019/20	Corporate inductions are completed for each new starter which includes them receiving an 'induction manual' which includes a number of the council's key policies and procedures, e.g. Code of Conduct, Data	An on-line training portal should be researched to ensure staff have access to the necessary training at the start of their employment. Modules should include Data Protection and Information Security.	Liesl Hadgraft / Steve Simpson On-going	Owing to the on-going pandemic, progress has slowed down. Observations of the Lancaster city Council training platform have been made, however a decision has yet to be made on if this software is considered

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
		Protection Policy etc. In 2018 all staff attended mandatory GDPR training. This was an interactive session carried out using an e-learning training package. This training package is now out of date and cannot be used, therefore there are a number of staff who have joined the council since 2018 that have received an induction pack but have not received any specific face-to-face GDPR and information security training. For this reason a number of staff will not sign the 'declaration of understanding' stating they have received, understood and will comply with the Data Protection Policy and Procedure.	A list of staff who have not received any GDPR / Information Security training and / or will not sign the 'declaration of understanding' form will be formulated. A decision will made if an alternative solution will be considered whilst a new training platform is procured.	Jo Billington Immediate	appropriate for the council. The DPO has formulated a list of all staff who have not received any training and/or have not signed the declaration of understanding. The Data Protection Policy has been updated to reflect the council's current arrangements for training new starters and refresher training for existing staff in these areas. On-going
Transparency Code	2019/20	The council endeavours to comply with the Local Government Transparency Code 2010 and publishes a number of documents on the website. However it was noted that not all the information was up to date and key documents were missing.	A full review of compliance to the Local Government Transparency Code needs to be completed.	Jo Porter September 2020	A review has been completed and responsible officers have been notified of any actions that are required to ensure compliance. A follow-up piece of work will be completed in the new year by the Information Governance Manager. **Completed**

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
Competency Framework	2019/20	A competency framework exists to ensure that all staff have appropriate skills to enable them to deliver high quality services. However it was noted that this document may need to be reviewed.	The Competency Framework needs to be reviewed, refreshed and rolled out corporately.	Liesl Hadgraft On-going	Owing to the on-going pandemic this has not been progressed any further. It is not known when this work will be completed due to key members of the Human Resources staff currently assisting with the Covid Test and Trace programme.
Performance Management	2019/20	Quarterly performance reports are submitted to the Overview and Scrutiny Committee. However it was identified that there is a lack of resources to look after the reporting process.	A review will be completed to ensure the necessary resources are allocated to support the performance management framework and that following the CMT restructure, it sits with the most relevant service.	Marianne Hesketh September 2020	Internal Audit are in the process of completing a piece of work to review the effectiveness of the council's performance management processes. A draft report will be issued in December 2020. The report will assist the Corporate Director align responsibilities and resources appropriately going forward.
IRP Member Training	2019/20	The Independent Remuneration Panel is now back to full capacity, with the new member attending their first meeting in November 2019. Whilst the new member does have a governance background, he has never sat on a similar panel or worked with elected members from a Local Authority.	Following a discussion between the Democratic Services Manager and the new IRP Member a decision will be made if training is required or indeed if there is any training available of this nature.	Peter Foulsham December 2020	Owing to the on-going pandemic the IRP meeting has been delayed until January 2021. The new IRP member is also an IRP Member at Lancaster City Council (LCC). The Head of Governance will liaise with the Democratic Services Manager at LCC to identify if any training will or has been provided there.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
Councillor Skills Framework	2019/20	Councillor Personal Development Plans (PDP's) have now been replaced with much simpler "Wyre Councillor Skills Framework" questionnaires which were agreed by the Councillor Development Group at their meeting on 9 March 2020. Owing to the Covid-19 pandemic, the circulation and completion of these has been delayed.	The questionnaire will be circulated to all councillors for completion once the council returns to some form of normality.	Duncan Jowitt Estimated – September 2020	Owing to the on-going pandemic this piece of work is still outstanding. The Democratic Services Team have been focusing on supporting both Elected Members and Officers with the move to fully remote meetings. This will be revisited in the new year. A survey which focuses more on the Health and Wellbeing impact of the pandemic on Councillors is to be rolled out this year instead.
Counter Fraud Policies	2019/20	The staff ethical governance survey that was carried out in October 2018 identified that a number of staff were unfamiliar with the Anti-Money Laundering Policy, The Anti-Fraud, Corruption and Bribery Policy and the Whistleblowing Policy and in some instances didn't know how to raise concerns or report suspected fraud.	Following the annual review at Audit Committee in November, the council's counter fraud policies will be refreshed and rolled out. Consideration will also be given to publishing ad hoc 'Fraud Bulletins' to ensure staff are kept up to date with changes to polices, legislation and any other information that can be shared in relation to recent investigations or outcomes.	Jo Billington / Andrew Robinson / Emma Lyons November 2020	The councils counter fraud polices (with the exception of the Anti-Money Laundering Policy) were reviewed by Audit Committee in November 2020 and will now be added to SharePoint. Owing to the Compliance Manage administering the Covid grants, no progress has yet been made in respect of the publication of a Fraud Bulletin. This will be considered when normal business resumes.
Statutory Roles	2019/20	The staff ethical governance survey that was carried out in October 2018	Consideration will be given as to how this issue will be addressed going forward.	Clare James / Liesl Hadgraft	Owing to the on-going pandemic this has not been progressed any further.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
		identified that a number of staff have either a 'poor' or are 'not aware' of the roles and responsibilities of some of the council's key officers; namely, the S151 and the Monitoring Officer.		December 2020	
Modern.Gov	2019/20	Following the purchase of Mod.Gov in 2019, the Council now holds paperless meetings. Templates for agendas and minutes are on Mod.gov, but at present report templates are not available. A much larger and complex piece of work (work flow implementation) will need to be completed to allow officers to write their reports on Mod.gov and circulate them for comment and amendment in a way that ensures that version control is strictly maintained. This is a medium-term project that will be time-consuming, and will come with additional costs, due to the Democratic Services Team requiring further training from the system administrators at Modern.Gov.	CMT need to approve the next stage of development of the Modern Gov application; Work Flow Implementation, in particular the additional costs that will be incurred due to further training required by the Democratic Services Team to ensure that the next stage can be delivered successfully and the council utilises the system to its full potential.	Peter Foulsham / CMT On-going	Owing to the on-going pandemic this has not been progressed any further. The Democratic Services Team have been focusing on supporting elected members and officers following the move to remote meetings. This will be revisited in the new year, following recruitment to the vacant DSO post.

Governance Issue	Year relating to	Finding	Action required	Timescales / Officer Responsible	Update as at November 2020
Corporate Comments, Compliments and Complaints Procedure	2019/20	The staff ethical governance survey that was 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, in particular, how the policy worked and where to locate it. There were also a number of staff who did not know where or who to go to for support or advice on this procedure.	The corporate Comments, Compliments and Complaints Procedure should be refreshed and rolled out to all staff to ensure they understand its content, the processes and stages involved and who to go to for support and advice. Consideration should also be given to including this in the corporate induction packs.	Peter Mason December 2020	Owing to the on-going pandemic this has not been progresses any further. This will be revisited in the new year.
YMCA	2019/20	The 2019/20 subsidy target is expected to be exceeded by c£250,000. However this was not reported to the council until the end of September 2019. A new pricing structure was introduced in 2019 and competition from new gyms in Wyre have contributed to the worsening position.	Meetings with the YMCA have been held to discuss the outturn and a contract variation for 2019/20 to allow for both parties to share the increased cost on a 50/50 basis. Prior to Covid-19 the YMCA were optimistic 2020/21 would see a recovery to the agreed subsidy level of £147,500 but this is now not possible. Further work is ongoing to support the YMCA's cashflow during the pandemic. Any significant changes will need to be approved.	Corporate Director Communities On-going	Following the recent pandemic which resulted in the closure of the Borough's leisure centres, the council has continued to financially support the YMCA. The CMT and Management Board are working closely with the YMCA to work through the pandemic. A report under emergency powers was approved during the first lockdown to agree additional funding of £489,000 for 2020/21. This situation is being kept under review.

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	26 November 2020

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/b4128/Proposed%20Financial%20Regulations%20and%20Financial%20Procedure%20Rules%2026th-Nov-2020%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 reviewed by the Corporate Director Resources. The

last review was completed in November 2019.

5. Key Issues and proposals

5.1 A number of amendments are proposed, namely:

- Amended to reflect that the 'Finance Director' is either the Corporate Director Resources or their nominated deputy acting in that capacity (Part 4.06/03 para 1.4e);

- Amended to reflect the changes to IFR16 that require all lease agreements to be notified to the Financial Services Team to ensure correct accounting treatment is followed (Part 4.06.04/9 para 3.61 - 3.62 & Part 4.06.05/6 para 4.44);

- The removal of the reference to the 'Wyre and Fylde Community Network' as an example of one of the many engagement network groups in the Borough (Part 4.06.06/16);

- Update the EU procurement thresholds which came into effect from January 2020 (Part 4.06.07/4); and

- Amended to reflect that for contracts exceeding the EU procurement thresholds the successful bidder should be notified promptly following acceptance of the tender or quotation with an Alcatel letter (Part 4.06.07/7).

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

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

health and safety	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	18.11.20

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 website available to view here: https://wyre.moderngov.co.uk/documents/b4128/Proposed%20Financial%20Regulations%20and%20Financial%20Procedure%20Rules%2026th-Nov-2020%2018.00%20Audit%20Committee.pdf?T=9).

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	26 November 2020

ANNUAL REVIEW OF THE COUNCIL'S COUNTER FRAUD POLICIES – ANTI-FRAUD, CORRUPTION AND BRIBERY, 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;
- 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 policy documents detailed above.

4. Background

4.1 The Audit Committee work plan includes an annual review of the policies listed below:

4.2 Anti-Fraud, Corruption and Bribery - originally approved by the Standards Committee in 2006. The policy was amended in November 2011 to make reference to the Bribery Act 2010, which came into effect on the 1 July 2011.

4.3 Whistleblowing - originally agreed by the Standards Committee in 2004. The Whistleblowing Policy has been reviewed using the British Standards Institute (BSI) Whistleblowing Arrangements Code of Practice for 1998:2008 and the Enterprise and Regulatory Reform Act (ERRA) which received royal assent on 25 April 2013. The ERRA includes major changes to employment law which will impact considerably on whistle-blower protection. The policy has also been reviewed to ensure it is in

line with the Public Concern At Work publication; The Whistleblowing Commission - Report on the effectiveness of existing arrangements for workplace whistleblowing in the UK, published in November 2013.

4.4 Gifts and Hospitality and Registering Interests – originally agreed by Audit Committee in February 2009.

5. Key Issues and proposals

5.1 The general aim of all the council's counter fraud 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.

5.2 The Whistleblowing Policy has been amended to correct the error with the council's whistleblowing email address (para 5.3), to reflect that the Section 151 Officer is now the Corporate Director Resources, not the Head of Finance (para 5.5, 8.1) and to note the change to the Public Concern at Work email address (para 7.1).

5.3 The Anti-Fraud, Corruption and Bribery Policy has been amended to reflect that the Section 151 Officer is now the Corporate Director Resources, not the Head of Finance (para 4.10) and the link to the Council's IT Computer Use Policy has been updated to reflect its new location in SharePoint (para 4.12).

5.4 The links in the Gifts and Hospitality and Registering Interest's Policy have all been updated to reflect their new location in SharePoint.

5.5 All the draft policies can be viewed by using the following link. Changes are highlighted in yellow.

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

5.6 The Anti-Money Laundering Policy and Procedure will be reviewed in January 2021 and submitted to the Audit Committee for approval in March 2021.

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
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	18.11.2020

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

List of appendices

None

This page is intentionally left blank

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	26 November 2020

APPROVAL OF THE COUNCIL'S DATA PROTECTION POLICY AND PROCEDURES

1. Purpose of report

1.1 Approval of the council's Data Protection Policy and Procedures which includes the council's incident / breach reporting and investigation instruction.

2. Outcomes

2.1 The ability to demonstrate that the council has arrangements in place to ensure compliance with the General Data Protection Regulations (GDPR) and other data protection laws.

3. Recommendation

3.1 Members are asked to approve the attached Data Protection Policy and Procedures and incident / breach reporting and investigation instruction at Appendix 1.

4. Background

4.1 In March 2018 the Audit Committee were given delegated responsibility for ensuring the council is complaint with the GDPR and other data protection law, e.g. the Data Protection Act 2018. The Committee's Terms of Reference states; "To receive updates and reports from the Head of Governance (Data Protection Officer) and to approve policies in relation to compliance with the Data Protection Act and Regulations made under the Act".

4.2 Wyre Council takes its responsibilities with regards to the management of the requirements of the GDPR and other data protection requirements very seriously. This policy sets out how the council manages those responsibilities.

4.3 The council obtains, uses, stores and processes personal data relating to our residents / customers, potential, current and former staff, contractors and partners, collectively referred to in this policy as 'data subjects'.

When processing personal data, the council is obliged to fulfil individuals' reasonable expectations of privacy by complying with the GDPR and other relevant data protection legislation (The Data Protection Act 2018).

4.4 This policy and guidance seeks to ensure that the council;

- is clear about how personal data must be processed and the expectations for all those who process personal data on its behalf;
- complies with the data protection law and with any other good practice around data processing;
- protects its reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights; and
- protects itself from risks of personal data breaches and other breaches of data protection law.

5. Key Issues and proposals

5.1 The Data Protection Policy and Procedures and incident / breach reporting and investigation instruction was last reviewed and approved by the Audit Committee in November 2019 and is attached at Appendix 1. Following a review by the council's Data Protection Officer, only one minor change, relating to the council's approach to Data Protection Training (para 16.2) has been made.

Financial and legal implications	
Finance	There are no specific financial implications arising from the adoption of this policy.
Legal	The council's Data Protection Policy and Procedures assist the council in ensuring it meets the requirements of the General Data Protection Regulations and other data protection law.

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	18.11.2020

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

List of appendices

Appendix 1 – Data Protection Policy and Procedures

Data Protection Policy and Procedures

Version 2.0 – November 2020

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 Council') recognises that compliance with data protection legislation (including the 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 Council 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 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 Council, 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.

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 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 Council's Constitution
- Employee's Code of Conduct
- ICT Computer Use Policy
- Security Incident Policy

- Records Management Policy
- Password Policy and User Guidance

4.0 Personal data processed by the Council

4.1 The Council 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 Council 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 Council 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 Council is a data controller will be communicated by the Council to data subjects by means of appropriate privacy notices.

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

4.4 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 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 Council has two registration numbers Z5682712 (General processing) and ZA319367 (elected Members); and
- Inform the ICO and in some instances the data subject of any data breaches.

5.0 Data protection principles

5.1 The Council will comply with the principles relating to the processing of personal data set out in the 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 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 Council shall be responsible for, and be able to demonstrate compliance with all the above principles.

5.3 Where the Council 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 Council 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 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 Council will ensure that one of the additional conditions set out in relation to special category personal data in the 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 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 Council 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 GDPR) the Council 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 Council'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 Council 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 Council 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 Council 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 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 Council 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 Council 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 Council 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 Council 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 Council will ordinarily refuse the request(s). In exceptional cases the Council 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 Council recognises the fundamental nature of the individual rights provided by data protection legislation. The Council 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 Council 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 Council's on-line process. However, a valid request may also be made verbally.

7.7 The Council'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 Council'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 Council 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 Council 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 Council, they may ask for the matter to be dealt with by the Council'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 Council 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 Council's intranet.

8.0 Individuals' Rights – Law Enforcement Processing

8.1 The rules relating to an individual's rights are different where the Council 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 Council is processing for law enforcement purposes the Council will ordinarily respond without undue delay and in any event within one calendar month. There is not an option for the Council to extend this for a further period in the case of complex or numerous requests, although the Council can refuse (or make an administrative charge for) manifestly unfounded or excessive requests.

9.0 Further legal requirements

9.1 The Council 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 Council 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 Council 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 Council ("data processors") must be required to demonstrate, via a written contractual agreement, that personal data belonging to the Council 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 Council and a data processor will contain all the relevant elements specified in data protection legislation.

9.4 The Council 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 The Council 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)

10.1 The Council'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 Council 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 Council will ensure that only personal data that is necessary for a specific purpose is processed. The Council 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 will need to be completed and signed off by the Council's DPO before the activity commences.

11.0 Records Management

11.1 The Council must manage and dispose of its records in accordance with the Council's Records Management Policy 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 Council 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 Council will process personal data in accordance with the DPA and GDPR and any other related Council 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;
- 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 Council'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 ICT for assistance if they are wanting to transfer personal data out of the organisation;
- Desktop 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 must be used for the destruction of personal data. The Council 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.

13.0 Information Sharing

13.1 When personal data is collected, the data subject must be informed, via a privacy notice, what data the Council 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 Council departments and with contractors working on the Council's behalf for legitimate purposes, such as:

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

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 Council's DPO.

13.4 Information sharing protocols / agreements should be in place between all Council and third parties when personal data is being shared. All agreements must be signed off by the DPO at which point a record of the data shared will be documented in the relevant information asset register.

13.5 Any sharing of Council-controlled personal data with other data controllers must comply with all statutory requirements and corporate policies. Where appropriate the Council 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 regularly. Any data sharing agreements must be signed off by the DPO and the Council'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.

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 if they do not know how to encrypt an email or a document that contains personal data.

14.3 Postal Mail
The Council 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 Council 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 Council has an Information Governance Group which is accountable for ensuring compliance with this policy across the Council. The work of the group will be supported by the Corporate Management Team and the Audit Committee who have delegated responsibility for ensuring the Council's compliance to the DPA and GDPR. The group's membership consists of the DPO, the Information Governance Manager (Deputy DPO), Head of ICT and the Legal Services Manager.

15.3 The Council will ensure that:

- The DPO reports to the highest management level of the Council in respect of their duties as DPO, in this instance, this is the Corporate Management Team.
- 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; and
- 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 Council systems may be used by Elected Members in their roles, the data controller may be the Elected Member or the Council individually, jointly or on behalf of the other. Notification must be arranged as follows:

- When acting on behalf of the Council, Elected Members can rely on the Council'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 GDPR; and
- 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 Council'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 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 Elected Members must attend all training recommended to them and take the necessary steps to ensure the Council's data is stored safely in accordance with any Council policy and procedure. They must store all Council data separately from data relating to their ward and political party work.

16.0 Training

16.1 The Council 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 Council is mandatory and Line Managers are responsible for ensuring that all staff attend and that staff are given the necessary time to attend. The Council provides all new starters with an induction pack which includes the Data Protection Policy and Procedures and Incident / Breach Reporting and Investigation Instruction. All staff are asked to sign to confirm they have read and that they understand the content of both documents. Whilst previously the Council used an e-learning video and tests to train all its staff on data protection and information security, access to this software is no longer permitted. At the time of this policy review, the Council was in the process of looking for a corporate e-learning training platform what would include both Data Protection and Information Security training modules.

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 Council'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 Council's intranet and also the Council'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 Council's 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 helpdesk	01253 887652 / 887425

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 Council'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 Council 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 The ICO recommends that 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.

4.4 For further information on the four steps detailed at 4.2, please refer to the Data Protection page on the Council's intranet 'carrying out an investigation'.

https://wyregovuk.sharepoint.com/sites/Governance/SitePages/Data-protection.aspx

Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	26 November 2020

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 - Practice 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 and agree the one area identified where further improvement is considered beneficial.

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 Head of Governance (Chief Internal Auditor) and reviewed by the Corporate Director Resources (Section 151 Officer). Members will be asked to contribute to a discussion at the remote meeting with a view to ensuring the Audit Committee are still meeting the requirements of CIPFA's 'Self-Assessment of Good Practice' and agree the one area that has been identified as requiring attention (Q4 - highlighted in bold).

Financial and legal implications	
Finance	There are no specific financial implications arising from the agreement of the improvement plan.
Legal	There are no specific legal implications arising from the agreement of the improvement plan.

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
Joanne Billington	01253 887372	joanne.billington@wyre.gov.uk	10.11.2020

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

List of appendices

Appendix 1 – CIPFA Self-Assessment of Good Practice

Appendix 1

CIPFA Self-Assessment of Good Practice – November 2020

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 14 November 2019.
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 have recently been revised (March 2019) to accurately reflect 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?		✓		The majority of the current membership have all received training on the role and purpose of the Audit Committee. However, following the Annual Meeting one new member has joined the Audit Committee and owing to the on-going pandemic training has not been given to this new member. Given emergency powers were introduced in April 2020, training the new member was not considered a priority. Remote meetings are now commencing

Good practice questions		Yes	Partly	No	Comments
					therefore training will be arranged. **<u>Action</u>** **The new Audit Committee member will receive training on the execution of their terms of reference. This may be virtual training, given the current working arrangements.**
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 compliance to the General Data Protection Regulations 2018.
6	Are the arrangements to hold the Audit Committee to account for its performance operating satisfactorily?	✓			A review of effectiveness is completed annually and discussed with the Audit Committee. An action plan is formulated of any issues that need attention. It should be noted that an annual review was not completed in November 2018 due to the local elections in May 2018 and given the Audit Committee had only met on three occasions at the time the annual review was scheduled.
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

Good practice questions		Yes	Partly	No	Comments
	▪ 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				Local Authorities and Police 2018'.
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 Head of Governance (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 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

Good practice questions		Yes	Partly	No	Comments
					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. Whilst the size of the Audit Committee has been discussed on a number of occasions, a decision has been made by the Leader of the Council to leave the current membership number (14) as it is.
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.
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.

Good practice questions		Yes	Partly	No	Comments
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. 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?	✓			Both the Corporate Director Resources (Section 151 Officer) and the Head of Governance (Chief Internal Auditor) attend every Audit Committee meeting, with the exception of the July meeting to approve the Statement of Accounts, which the Head of Governance does not attend. Also a representative from our 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

Good practice questions		Yes	Partly	No	Comments
					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 'weak' overall assurance opinion, the Audit Committee will make recommendations for further audit review, more frequent updates and may also request the intervention of the relevant Director or Portfolio Holder for additional assurances that the weaknesses are being addressed i.e. Marine Hall.
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 organsiation.
24	Does the Audit Committee have an action plan to improve any areas of weakness?	✓			Actions contained within this checklist are highlighted in bold and will be implemented prior to the next annual 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 the 14

Good practice questions		Yes	Partly	No	Comments
					November 2019. The report explains the work of the Committee and more specifically details the reports that been submitted to the Audit Committee during the year.