Risk Management Policy and Framework

June 2020
Version 1.05
(Update for Governance, Risk and Audit Committee – June 2020)

Foreword

The fundamental principles adopted by the Council on risk management are described within the policy statement and adopting and implementing the strategy detailed below will achieve compliance with the policy.

Review of the policy follows a recent assurance review of risk management (NN/20/10), the objective of the audit was to review the systems and controls in place within the risk management systems, to ensure they are operating adequately, effectively and efficiently and to recommend any areas for improvement. As part of the audit process this document was also reviewed.

The audit concluded that the systems and processes of internal control are deemed 'Substantial' in managing the risks associated with the audit. The previous report on Risk Management (NN/18/14) was issued in March 2018 and resulted in the same opinion. This indicates that we have maintained a high level of assurance and that the system of controls has continued to operate well since the previous audit.

Since the previous policy statement was adopted the authority has strengthened the risk management framework in a number of areas and will continue to do so in line with the improvements to the Project Management framework and wider governance processes.

Improvements include the following;
- Quarterly review of the Corporate Risk Register by the Senior Leadership Team (SLT) where there was previously no regular programmed oversight;
- Quarterly review of the Corporate Risk Register by the Governance, Risk and Audit Committee (GRAC) where previously this was only undertaken every 6 months;
- Member training on risk undertake on 6 February and 5 March 2020;
- Workshops held with SLT, Cabinet and wider Members to establish the Council's risk appetite;
- Improvements to the Council's Project Management framework supported by improved risk management processes;
- Ongoing transfer of the risk registers to the Council's new performance monitoring system 'InPhase';
- Enhanced risk assessment processes built in to the Medium Term Financial Strategy (MTFS) and 2020/21 budget;
- Improvements made to the Council's Corporate Risk Register to include;
  - Identification of a single 'risk owner'
  - Identification of appropriate officer(s) to progress mitigation actions
  - Target dates for completion of mitigations

Without a robust risk policy and framework the Council is at risk in a number of areas. Setting the Council's risk appetite will help to inform and support decision making as we deliver the aspirations contained within the new Corporate Plan and Delivery Plan.

Contents

Policy Statement

This policy will take effect from the date of approval (Governance, Risk and Audit Committee). It is the policy of the Council to adopt a proactive approach, through its management processes, to risk management of the services it delivers both for itself and in partnership with others.

It is recognised that a certain amount of risk is necessary and indeed that it can be a positive force in the development of the services we provide. However, this needs to be managed in order to:-

- Safeguard our clients or service users, Members and employees and all other persons to whom the Council has a duty of care

- Ensure compliance with statutory obligations

- Preserve and enhance service delivery

- Protect our property, including buildings, equipment, vehicles and all other assets and resources

- Maintain effective control of public funds

- Protect and promote the reputation of the Council

- Support the quality of the environment

- Achieve the objectives in the Corporate Plan, Delivery Plan and Service Plans

- Safeguard the information we hold, obtain, record use and share based on the new General Data Protection Regulations (GDPR)

All of these objectives will be achieved by applying the Council's risk management strategy, which outlines responsibilities for managing risks and defines how risk management should be applied across the Council.

The master copy of this document, a record of review and decision making processes will be held by the Head of Finance and Assets.

This policy will be available to all staff and Members on the corporate document register on the intranet.

2. Strategy Background

All organisations face a wide variety of risks including physical risks to people or property, financial loss, operational risks and failure of service delivery, macroeconomic issues, credit and counterparty investment risk, strategic risks to the organisations objectives, environmental and social risks, along with governance and reputational risks. Risk for this purpose is defined as "the chance of an event

happening and leading to unintended effects which will impair the organisation's ability to achieve its objectives".

Risk management is intended to be a planned and systematic approach to the identification, assessment and management of the risks facing the organisation.

The traditional means of protecting against the more obvious risks has been through insurance. However, there are many risks which cannot be insured against and which must be addressed in different ways. Even in the case of those risks which are insurable, action can be taken to reduce the potential risks with consequent savings of premiums and disruption of work.

The risk management strategy aims to:-

- Clarify responsibilities for identifying and managing risks

- Ensure that an appropriate level of risk management is consistently applied across the Council

- Increase awareness and use of risk management as a normal element of service management and improvement

- Facilitate sharing of experience and good practice across the Council and with other bodies

3.   Leadership and Responsibility

Given the diversity of Council services and the wide range of potential risks, it is essential that responsibility for identifying and taking action to address potential risks is clear.

Responsibility for effective risk management rests with all Members and Officers of the Council.

The Corporate Director and Head of Paid Service is the Officer with overall responsibility for securing adherence to the Council's policy on Risk Management. The Head Of Legal is designated as the Council's Senior Risk Information Officer (SIRO) and will take overall ownership of the Council's Information Risk Policy, act as champion for information risk on the Strategic Leadership Team and provide written advice to the Head of Finance and Assets on the content of the Council's Statement of Internal Control in regard to information risk.

The framework of roles and responsibilities in Appendix One shows how these are allocated.

4.   Corporate Governance

North Norfolk District Council has adopted a Local Code of Corporate Governance setting out the framework through which it will carry out its responsibilities to deliver

effective services.

Core principle four requires "taking informed and transparent decisions which are subject to effective scrutiny and managing risk". This requires that an effective risk management system is in place.

As part of the Local Code it states that the authority should prepare and publish an Annual Governance Statement (AGS). This statement is a key corporate document and will include an assessment of the authority's effectiveness of managing risk; it is signed by the Corporate Director and Head of Paid Service and Leader of the Council.

The assessment of the authority's effectiveness of managing risk is provided by an annual report to the Governance, Risk and Audit Committee (GRAC).

To enable links to be made to the Corporate Plan and Delivery Plan, the Corporate Risk Register (CRR) identifies the Corporate Objective / Service priority to which that risk is identified.

5.   Resourcing Risk Management

Risk management is not a new issue and, as identified in the Leadership and Responsibility Section, every Member and Officer is responsible for considering risk implications as they relate to their actions. Since the adoption and implementation of the Risk Management Framework in 2010 the concept of risk management has been formalised and is part and parcel of the culture of the Council.

The designated Risk Champion(s) at Management Team Level is the Head of Finance and Assets who also covers the role of Corporate Risk Officer.

Information Technology is used in the form of the InPhase Performance and Risk System, which includes a dedicated risk module

6.   Officer and Member Roles

Whilst acknowledging the wide variety of risks that face the Council, and the differing circumstances that apply in different services, it is essential that there is some consistency in the way that risks are identified and assessed. This helps to ensure that all areas of risk are adequately considered and relative priorities for action can be judged.

The Risk Management Board that had previously managed risk on behalf of the authority and been replaced by risk management being embedded at service level and project management level for less significant risks and the Corporate Risk Register being managed by Strategic Leadership Team and GRAC.

The Corporate Risk Register is a standing item on the agenda (for any issues or changes that arise) at every GRAC meeting and is considered and reviewed by SLT on a quarterly basis.

SLT acts as a link between service managers, specialised groups dealing with particular areas of risk and Members.

7. Risk Management Role in the Cabinet and Governance, Risk and Audit Committee

The Cabinet is responsible for ensuring that an adequate risk management framework and associated control environment exists within the Council.

The Audit Committee was established in 2006 but has now been replaced by the Governance, Risk and Audit Committee. This Committee is responsible for monitoring the arrangements in place for the identification, monitoring and management of strategic and operational risk.

To provide the Governance, Risk and Audit Committee with the necessary information to undertake these responsibilities, regular progress updates on the Corporate Risk Register are reported at every meeting.

8. Risk Management Approach

The development of a consistent, corporate approach to risk management is done in a methodical and proportionate way in order to avoid the creation of a self-defeating bureaucratic burden.

To ensure that risk management is handled in the most efficient way within the Council, the risk element has been included in the Service Plans and the work to implement the risk management strategy has been included in the InPhase Performance and Risk System.

9. Methodology

A methodology for identifying, assessing and managing risk within the Council is in operation. This methodology has the advantage of being relatively straightforward to use and can be applied to both the strategic risks of the Council and as part of the routine service and project planning processes.

Guidance for managers on the application of the risk management methodology has been produced and is embedded in the InPhase Performance and Risk System. Risk review meetings between the Policy and Performance Management Officer and Service Managers are held at least every six months to review and updated the assessment of existing risk and their management, to identify new risks and risks that should be put forward for inclusion in the Corporate Risk Register (CRR). Processes have also been improved in respect of individual risk registers whereby any risk classified as 'high' is escalated for inclusion within the CRR.

Risk assessments should be produced to support strategic policy decisions and all

major projects. The Guide to Project Management (on the Intranet) includes how to assess risk and has forms to capture the data. The Council's risk management methodology should be followed to produce these risk assessments and a summary of the findings given in reports to Members.

Risk management training will be provided for managers to assist with implementing the risk management methodology. Managing Risk is a tutorial in the e-learning portal.

10.   Risk Scoring, Matrix and Risk Tolerance

Corporate Risks

Each corporate risk (a similar matrix is used for service risks) will be assessed against the following criteria:

Corporate Risk					
Impact Type	**Catastrophic 5**	**Critical 4**	**Moderate 3**	**Marginal 2**	**Negligible 1**
Objectives	The key objectives in the Corporate Plan will not be achieved.	One or more Key Objectives in the Corporate Plan will not be achieved.	Significant impact on the success of the Corporate Plan.	Some impact on more than one Service.	Insignificant impact on more than one Service.
Financial Impact (Loss)	Over £1.5m	£500K - £1.5m	£300K - £500K	£20K - £300K	£0-20K

Likelihood ratings and dimensions are tabled below

Grade	Likelihood	Probability	Timing
5	Very High	Over 90%	Within six months
4	High	60 - 90%	Within a year
3	Moderate	40 - 60%	Within 1 to 2 years
2	Low	10 - 40%	Probably within 15 years
1	Very Low	below 10%	Probably over 15 years

Instructions issued with service plans

Impact ratings and dimensions are tabled below.

Service Risk

Impact Type	Catastrophic 5	Critical 4	Moderate 3	Marginal 2	Negligible 1
Objectives	The key objectives in the Business Plan will not be achieved	One or more Key Objectives in the Business Plan will not be achieved.	Significant impact on the success of the Service Business Plan.	Personal or team objectives not met.	Insignificant impact.
Financial Impact (Loss)*	Over £500K	£300K - £500K	£75K - £300K	£10K - £75K	£0-10K
Service provision	Service suspended long term or statutory duties not delivered.	Service suspended short term.	Service reduced significantly	Slightly reduced	No effect

* Note: these are indicative figures it may be better to use % of budget for some of the smaller services.

Likelihood ratings and dimensions are tabled below.

Grade	Likelihood	Probability	Timing
5	Very High	Over 90%	Within six months
4	High	60 - 90%	Within a year
3	Moderate	40 - 60%	Within 1 to 2 years
2	Low	10 - 40%	Probably within 15 years
1	Very Low	below 10%	Probably over 15 years

The probability and timing are guidelines only and should be used with judgement. For example: an identified risk happened in the last six months but had not occurred previously for over 10 years. The likelihood of it happening again is still probably still Low, particularly if you feel that any new controls put in place since the risk happened have made it less likely.

Risk Matrix

The scoring by using a 5x5 matrix, which multiplies the numbers together, gives a wider range of scores.

Matrix

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Multiply	**1**	**2**	**3**	**4**	**5**

Likelihood of occurrence

Severity of impact / consequences

A very high likelihood with a catastrophic impact would score 25 but something that was very low likelihood and negligible impact would only score 1.

Risk Tolerance

Matrix

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Multiply	**1**	**2**	**3**	**4**	**5**

Likelihood of occurrence

Severity of impact / consequences

A score of 6 or under is deemed marginal and requires no further action. A score of between 7 and 14 is deemed moderate and requires action to reduce the score. A score of over 15 is deemed critical and requires immediate action.

11.   Risk Appetite

Risk appetite is often described as "the amount of risk an organisation is willing to accept in the pursuit of their objectives". It is important to establish an organisations risk appetite for a number of reasons;

- No organisation can achieve its objectives without taking risks;
- A clearly articulated risk appetite empowers officers and Members to take appropriate risks to make the organisation successful;
- Risk appetite provides a boundary around the amount of risk an organisation might pursue;
- Encourages more "risk based" decision making to consider challenges and opportunities that arise and;
- Supports good governance - decision making.

As mentioned above risk appetite describes the amount of risk we are willing to take to achieve our objectives, risk tolerance is the degree of variance from our risk appetite which we are willing to tolerate as shown within the diagram below.
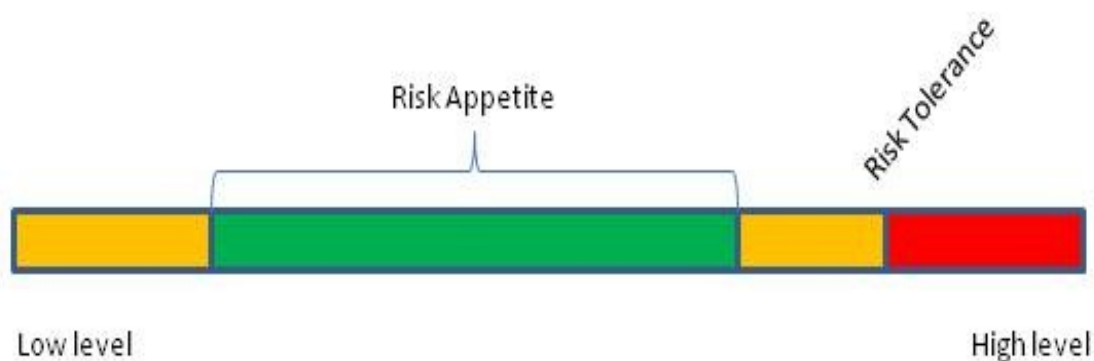
Following risk training and workshops with Members work has been undertaken to establish the Council's risk appetite which is a new area for the Council. This provides a further level of assurance so that both officers and Members have a shared understanding of the boundaries within which they are working.

Sessions were held with officers and Members to discuss the Council's risk framework and risk appetite on 6 Feb and 5 March 2020. Further sessions were then held with SLT and Cabinet. The feedback and general views from these sessions has been distilled into some overarching comments to help describe our risk appetite in various areas outlined below and this will be incorporated into the Corporate Risk Register in the future.

Risk	Appetite
Financial	High appetite for a range of asset classes, property and longer-term investments, subject to careful due diligence and an emphasis on security as well as matching with the Council's required liquidity profile. High appetite for high volatility investments as long as this is within a balanced portfolio so that the overall risk exposure is minimised. Medium risk for consideration of emerging markets with a lower appetite for capital growth oriented investments versus income generating investments. No appetite for currency risk.
Macroeconomic	High appetite for exposure to local and national economic growth. No appetite for exposure to global growth, interest rate risk, inflation risk, geopolitical and tail risk events.
Credit and counterparty	High appetite for exposure to highly rated counterparties, investment grade or secured credit risk and financial institutions with strong balance sheets, all subject to careful due diligence and an assessment of the transaction versus the Council's resources, capacity, funding needs, broader goals and cash flow requirements. No appetite for unsecured non- investment grade debt.

Operational	Medium appetite for BAU (Business as Usual) operational risks with staff empowered to make decisions. Low appetite for operational risks such as pricing errors, errors in administration, IT, cybersecurity etc. The Council maintains Risk Registers for key initiatives and significant investments to assess and mitigate specific risks on a more granular level. Business continuity plans have also been established to mitigate external occurrences. No appetite for fraud, regulatory breaches and exceeding risk tolerances.
Strategic	High appetite for strategic initiatives, where there is a direct gain to the Council's revenues or the ability to deliver its statutory duties more effectively and efficiently. Low appetite for initiatives and projects which sit outside of the Corporate Plan and Delivery Plan.
Environmental and Social	No appetite for environmentally negative risks or for social risks eg income, education, employment, health and housing, especially in the local region.
Governance	Low risk appetite in respect of compliance with Council policies, alignment with the Corporate Plan, delegation levels, fraud, transparency and major organizational change programmes. Medium appetite for partnership related risks.
Reputational	High risk appetite in respect of national media coverage, medium risk appetite for local media coverage and no risk appetite where social media and internal reputation are concerned.

It is recognised that a certain amount of risk is inherent in all of our activities and that it can be a positive driver in the development of the services we provide and our approach to investment.

To facilitate the delivery of our risk appetite, the risk management strategy sets out an approach for risks that are assessed as 'high' or 'very high' i.e. above a tolerable level. These are those risks that fall within the orange and red sections of the matrix.

It is helpful to include a broad overarching easily understood statement which encapsulates our current risk appetite level and possibly where we feel we need to move to and these can be seen within the table below.

Averse	Prepared to accept only the very lowest levels of risk, with the preference being for ultra-safe delivery options, while recognising that these will have little or no potential for reward/return.
Cautious	Willing to accept some low risks, while maintaining an overall preference for safe delivery options despite the probability of these having mostly restricted potential for reward/return.
Moderate	Tending always towards exposure to only modest levels of risk in order to achieve acceptable, but possibly unambitious outcomes.

Open	Prepared to consider all delivery options and select those with the highest probability of productive outcomes, even when there are elevated levels of associated risk.
Hungry	Eager to seek original/creative/pioneering delivery options and to accept the associated substantial risk levels in order to secure successful outcomes and meaningful reward/return

It is recommended that an appetite of "moderate" is adopted.

12. Risk Identification

To meet the requirements of this framework, risk(s) must be capable of being identified at any level, and by anybody, within the Council.

The key people are the service managers who will be actively monitoring their service plan to identify risks and change management practices and controls to reduce their impact. They can also be escalated to being a corporate risk through SLT.

13. Risk Registers

The authority has three levels of risk register. The Corporate Risk Register (CRR) which is maintained by the Corporate Risk Officer (Head of Finance and Assets) and monitored by SLT and GRAC. The service risks are monitored through the service plans and recorded on the InPhase system. There are also individual risk registers for certain projects such as the re-provision of leisure facilities in Sheringham. Reviewing service risks is the responsibility of the service manager with the support of the Policy and Performance Management Officer.

There is no "classic" definition of corporate risk as each organisation is different, however, as a guide a risk that would be described as corporate is one that would adversely affect the delivery of the Corporate Plan or mean the failure to deliver a corporate objective or affects more than one area of operation.

The Corporate Risk Register (CRR) is in the following format:

Name/No	Existing Controls	Score (with controls)	Action	Action Owner	Due date	Target Score	Risk Owner
1. Cause of risk 2. Description of Risk or potential event 3. Consequence of risk happening	Controls already in place	Impact x Likelihood = Total	To achieve target score	Officer responsible for undertaking any necessary actions	The date by which any mitigating actions are due	Impact x Likelihood = Total	Officer in overall charge of risk

The method of scoring likelihood and impact is in section 10. Similarly, there is no "classic" definition of service risk and it is the clear intention to only collect and monitor the main risks that face a service. In a similar way to the corporate risk, a

service risk is one that would adversely affect the delivery of the services business plan or mean the failure to deliver a service objective or affects more than one area within the service.

The service risks are gathered in a similar way:

Ref	Description of risk/ opportunity factor 1. Cause of risk 2. Description of risk 3. Consequence of risk occurring	Existing controls in place to reduce the risk.	Risk Score		Action to reduce risk score with timescale and responsible officer	Action owner	Due date	Target Score		Affected Corporate Objective or Service Activity
			I	L				I	L	

All service plans will have the risk element completed and signed off by the relevant Head of Service. For each risk the category or categories of risk are identified to assist in assessing the kind of control, mitigation and contingencies that should be put in place.

Categories of risk;

A Financial
B Macroeconomic
C Credit and counterparty
D Operational (including capacity/delivery/resources/health & safety)
E Strategic
F Environmental and Social
G Governance
H Reputational

The InPhase Performance system will show risks by service and risks and controls must be reviewed on a regular basis, the framework requires a six monthly update which will be facilitated by the Policy and Performance Management Officer.

Where service risks are highlighted as 'high risk' these will be escalated by Service Managers to the Corporate Risk register and monitored within InPhase.

14. Involvement of Other Related Groups

There are a number of other officer groups in existence which deal with specific areas of risk management. These include both the Health and Safety Group and the Corporate Business (Service) Continuity Group. These groups are represented at SLT by the various Heads of Service so that their work can be coordinated with the overall management of the risks facing the Council.

In addition to the groups listed above, the Council's Internal Audit section also contributes to the management of risk. The work of Internal Audit is based on a needs and risk assessment process that identifies and focuses resources on higher

risk areas. Audit findings are reported to the relevant Chief Officer and Service Manager together with recommendations for improvement and an action plan. Checks are undertaken by Internal Audit to ensure agreed recommendations are implemented.

The Corporate Risk Officer will receive copies of all finalised internal and external audit reports to assess if any change is required for the risk registers.

15. External Contacts

The potential risks faced by the Council are in many cases similar to those faced by other authorities and it is practical and cost effective to learn from the experience of others.

In order to share risk management information and experiences, the Council has established networks with other authorities and agencies. Specifically, the Council is a member of the Norfolk Risk Managers' Group. This Group, whose members include local authorities, police authority and others from Norfolk, meets on a regular basis to discuss risk management issues that are common to organisations and to share examples of best practice.

16. Linked Policies

There are a number of policies that are or will be linked to this framework:

Health and Safety Policy	IT Security Policy
Information Management Strategy	Business Continuity Policy
Information Risk Policy	Data Protection Policy

17. Review Process

This Framework will be reviewed by the SLT and any amendments will be agreed by the Governance, Risk and Audit Committee.

Appendix 1: Shared Leadership – Role and Responsibilities

Everyone has a role to play in an integrated risk management framework. Combining shared leadership with a team approach will help contribute to its ultimate success. Roles as identified at present are:

1.   FULL COUNCIL

Overall oversight of the Corporate Risk Management Framework.

2.   CABINET

To provide leadership and direction for the Council. To keep the Council's policies and objectives under review, including the Council's corporate strategic risks, and agree a programme of risk reduction where appropriate.

Receive progress reports on risk reduction programme as required.

Assess risks attached to proposals for new / changed policies and service delivery arrangements and make recommendations to Full Council.

3.   GOVERNANCE, RISK AND AUDIT COMMITTEE

Monitor to ensure that an adequate risk management framework and associated control environment is in place including the approval of the Corporate Risk Management Framework which includes the Policy Statement and Strategy.

Monitor arrangements for the identification, monitoring and management of strategic and operational risk within the Council

Receive progress reports on the corporate risk register at each meeting.

4.   CORPORATE DIRECTOR AND HEAD OF PAID SERVICE

Overall responsibility for securing adherence to the Council's Policy on Risk Management, including the Head of Legal having designation as the Council's Senior Risk Information Officer (SIRO) The description and responsibilities of this role can be found on the intranet.

5.   SENIOR LEADERSHIP TEAM (SLT)

Appoint a Head of Service and Member to jointly take responsibility for risk management.

Agree the Corporate Risk Management Framework including the Policy Statement and Strategy.

Consider risks attached to proposals for new / changed policies and service delivery arrangements.

Ensure that this framework is applied.

6.   CORPORATE HEALTH AND SAFETY GROUP

Reports directly to SLT and is charged with delivering health and safety policy across the Council.

7.   CORPORATE RISK OFFICER

Coordinate risk management activity across the Council

Report on risk management activity to the Senior Leadership Team (SLT) and Members.

Maintain a corporate risk register and liaise with Service Managers relating to service risks. Ensuring that the service risks are update on the risk system every six months.

Provide risk management training for officers and Members, appropriate to their needs and responsibilities.

8.   INDIVIDUAL SERVICE MANAGERS

Develop action plans in relation to corporate strategic risks as they relate to their area.

Identify risks attached to proposals for new / changed policies and service delivery arrangements.

Ensure that a service risk register is maintained and updated every six months on the risk system and that action plans are implemented.

9.   EMPLOYEES

Maintain awareness of risk management principles and take responsibility for managing risk within their own working environment.

Apply risk management to those risks requiring further action, particularly new developments and "project" work.

Maintain a record of risk assessments undertaken relating to them and any resulting action plans.

10.   INTERNAL AUDIT

Reporting to Management on the organisations performance under the Risk Management Framework.

11.   EXTERNAL AUDIT

Reporting to Management via Use of Resources etc on the organisations performance on risk management.

Document Information and Version Control

Document Name	Risk Management Policy and Framework
Document Description	The framework outlines responsibilities for managing risks and defines how risk management should be applied across the Council.
Document Status	Under Review
Lead Officer	Duncan Ellis
Sponsor	Steve Blatch
Produced by (service name)	Finance
Relevant to the services listed or all NNDC	All
Approved by	
Approval date	
Type of document	Policy and Framework
Equality Impact Assessment details	Not required
Review interval	Every 2 years
Next review date	

Version	Originator	Description including reason for changes	Date
1	Peter Gollop		August 2010
1.01	Helen Thomas	Transferred to policy template	23 October 2015
1.02	Helen Thomas	Marked up version showing out-of-date elements and suggested changes	09/11/2015
1.03	Karen Sly	Draft refresh presented to Audit Committee pending further review	February 2016
1.04	Duncan Ellis	Updated provided to the Governance, Risk and Audit Committee	March 2017
1.05	Duncan Ellis	Updated provided to the Governance, Risk and Audit Committee	March 2018
1.06	Duncan Ellis	Updated provided to the Governance, Risk and Audit Committee	June 2020