Appendix A

INFORMATION MANAGMENT RISK

POLICY

Author	Kevin McEvoy / Donald Ford
Department	Information Governance
Policy Owner	Head of Information Governance
Authoriser	Bayo Dosunmu, Senior Information Risk Officer
Published Date	
Version	4.2
Copies To	
Classification	Internal Use Only

Revision History

Version	Date	Revision Author	Summary of Changes
4.0	16/06/2021	Donald Ford	Revised version (items 1 to 11)
4.1	17/06/2021	Donald Ford	Amended item 10 (Risk Register)
4.2	27/07/2021	Donald Ford	Incorporating comments from Risk Manager and HR

Distribution

Version	Name	Position	Data Circulated
4.0	Matt Ginn	DPO / Head of IG	June 16, 2021
4.0	IG Team		June 16, 2021
4.1	James Rimmington	Risk Manager	June 28, 2021
4.2	Busola Osibogun	Head of HR	July 12, 2021

Approval

Name	Position	Date of Approval
Bayo Dosunmu	SIRO and Strategic Director of Residents Services	November 30, 2021

CONTENTS

Information Management Risk Policy

Lambeth Council 's Risk Policy Statement

LONDON BOROUGH OF LAMBETH RECOGNISES AND ACCEPTS ITS RESPONSIBILITY TO MANAGE RISKS EFFECTIVELY IN A STRUCTURED MANNER IN ORDER TO ACHIEVE ITS OBJECTIVES AND ENHANCE THE VALUE OF SERVICES PROVIDED TO THE COMMUNITY

1. Introduction

1.1 This policy details information risk management for Lambeth Council (LBL) and sets out the principles that the Council uses to identify, assess, and manage information risk, to support the achievement of its planned objectives, and aligns with the overall Council risk management framework and approach.

1.2 This policy demonstrates that information risk is a shared responsibility across Lambeth Council and is not the sole responsibility of ICT and Information Governance.

1.3 This high-level Information Risk Management Policy sits alongside the Information Security Policy and Data Protection Policy to provide the high-level outline of and justification for the Council's risk-based information security controls.

1.4 Consistent, high quality, timely and comprehensive data is vital to support good decision making and the delivery of improved service outcomes for LBL customers.

1.5 LBL relies on its information to be captured, stored, processed by its information systems to support and enable business processes and service delivery to achieve its strategic and operational objectives.

1.6 Information held by LBL must be recognised as a valuable asset, requiring appropriate levels of protection in accordance with its value to the organisation.

1.7 The following are requirements of LBL's approach to information risk management:

- 1.7.1 Create accountability for information risks at senior level, ensuring that the information governance model is discharged by all designated and/or nominated roles.

- 1.7.2 Enable service areas to take ownership in the identification, assessment, and management of information risks.

- 1.7.3 Ensure that information risk tasks are undertaken at strategic and operational levels.

- 1.7.4 Ensure that information risk management activities are executed in a timely and effective manner.

- 1.7.5 Ensure that Information Asset Owners (IAOs) provide assurance to the SIRO on information risks within their directorates as required.

2. Objectives

LBL's information risk management objectives are that:

- 2.1 Our information risks are identified, managed, and treated according to an agreed risk tolerance.
- 2.2 Our physical, procedural, and technical controls are agreed by the information asset owner
- 2.3 Our physical, procedural, and technical controls balance user experience and security.
- 2.4 Our physical, procedural, and technical controls are cost-effective and proportionate.

3. Scope

The Information Risk Management Policy and its supporting controls, processes and procedures apply to all information used within and by Council, in all formats. It applies to all individuals and other organisations who have access to LBL's information and technologies. It applies to those who process personal data in their dealings with LBL and external partners.

4. Compliance

4.1 Compliance with the controls in this policy will be monitored by the Information Governance Team and Information Security team and reported to the Serious Information Risk Owner.

4.2 All staff (including temporary and interim) and Elected Members are responsible for complying with this and other relevant policies and procedures covering the use and security of all information and personal sensitive or confidential information.

4.3 All LBL contractors, consultants, partners, or other agents must understand the value and sensitivity of LBL's information, treat it in accordance with this policy and ensure that their staff, who may have access to personal information held or processed for or on behalf of LBL, are aware of this policy and are fully trained in and aware of their duties and responsibilities under UK GDPR and Data Protection Act 2018.

5. Review

A review of this policy will be undertaken by the Information Governance team annually or more frequently as required and will be approved by the Senior Information Risk Owner where necessary.

6. Information Risk

6.1 Information risks typically fall within one of three categories:

- 6.1 .1 **Confidentiality**

  Ensuring only properly authorised persons can access information and controls are in place and operated which prevent unauthorised access.

- 6.1.2 **Integrity**

  Assessing the authenticity, accuracy, and completeness of data during its life cycle.

- 6.1.3 **Availability**

  Assuring that properly authorised people can access the information when they need to, at the right time and in the right ways.

6.2 Further details of the above and examples of common breaches of the above are set out in **Appendix 1.**

6.3. In addition, it is the responsibility of LBL to ensure that the information it holds is processed in accordance with data protection principles, rights, and obligations, ensuring its fair and responsible use. The information risk management process supports service areas in the identification, assessment, and management of privacy risks.

7. Risk assessment

7.1 Information Asset Owners must complete risk assessments of their information assets and processes on an annual basis, with access to and an understanding of:

- Lambeth Council's business processes.
- The impact to the Council of risks to business assets.
- The technical systems in place supporting the business.
- The legislation to which the Council is subject.
- Up-to-date threat and vulnerability assessments.

7.2 In addition, a risk assessment exercise must be completed at least:

- For every new information-processing system
- Following modification to systems or processes which could change the threats or vulnerabilities
- Following the introduction of a new information asset
- When there has been no review in the previous three years

7.3 A risk score is calculated from Likelihood x Impact Level, consistent with LBL's high level Risk Assessment Matrix. LBL's Risk Appetite Statement and Risk Assessment Matrix are set out in **Appendix 2** and LBL's Risk Appetite Thresholds are set out in **Appendix 3**.

8. Threats

8.1 LBL will consider all potential threats applicable to a particular system, whether natural or human, accidental, or malicious.

8.2 LBL will reference Annex C of the ISO 27005 standard to aid with threat identification.

8.3 Threat information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, and contacts across the sector and region.

8.4 It is the responsibility of the Information Security Team to maintain channels of communication with appropriate specialist organisations.

9. Vulnerabilities

9.1 LBL will consider all potential vulnerabilities applicable to a particular system, whether intrinsic or extrinsic.

9.2 LBL will reference Annex D of the ISO 27005 standard to aid with vulnerability identification.

9.3 Vulnerability information will be obtained from specialist security consultancies, local and national law enforcement agencies and security services, technology providers and contacts across the sector and region.

9.4 It is the responsibility of the Information Security Team to maintain channels of communication with appropriate specialist organisations.

10. Risk Register

10.1 The calculations listed in the risk assessment process will form the basis of the appropriate risk register. All risks, whether held within the Corporate Risk Register or within the relevant Divisional Risk Register, will be assigned an owner and a review date.

10.2 The Corporate Risk Register is held in the JCAD risk software with access controlled by the Risk and Insurance Team within the Directorate of Finance and Investment. The Corporate Risk Register records risks relating to corporate health, key processes, key people and key systems and strategic risks, that is risks that relate to strategic priorities and the Borough Plan. Business Unit level risks or project risks are recorded on the relevant Divisional Risk Register.

11. Risk Treatment

11.1 The risk register will include a risk treatment decision. The action will fall into at least one of the following categories:

- **Tolerate:** monitor to ensure the impact and likelihood do not change.
- **Treat:** introduce controls to reduce the impact/likelihood of the risk.
- **Transfer:** by insuring against the risk or passing to third party.
- **Terminate:** stop doing the activity that creates the risk (if possible).

"Tolerate" the risk refers to where the risk is within LBL's risk appetite and further treatment is not proportionate.

"Treat" the risk is where the risk is above LBL's risk appetite, but treatment is proportionate; or where the treatment is so simple and cost effective that it is proportionate to treat the risk even though it falls outside LBL's risk appetite.

"Transfer" the risk is where the risk cannot be brought below LBL's risk appetite with proportionate treatment, but a cost-effective option is available to transfer the risk to a third party.

"Terminate" the risk is where the risk cannot be brought below LBL's risk appetite with proportionate effort/resource and no cost-effective transfer is available.

11.2 Information Governance and the Information Security team in collaboration with the Information Asset Owner will review Medium and Low risks and recommend suitable action.

11.3 The Senior Information Risk Owner, Information Governance, and the Information Security in collaboration with the Information Asset Owner will review High risks and recommend suitable action.

11.4 In the event that the decision is to Treat, then additional activities or controls will be implemented via a Risk Treatment Plan.

12. Roles and Responsibilities

12.1 **The Senior Information Risk Owner (SIRO)** is a Strategic Director reporting to the Chief Executive Officer and is a member of the Council's most senior Management Board, chaired by the Chief Executive, with overarching responsibility for information risk policy.

12.1.2 The SIRO is accountable for information risk across Lambeth Council and ensures everyone is aware of their personal responsibility to safeguard and handle personal data in accordance with data protection legislation.

12.2 **Information Asset Owners (IAOS)** are responsible for information risk management within their directorate. Their role is to understand and address risks within their directorates, and to provide regular assurance to the SIRO that risks associated with the use of information assets have been scored and treated in accordance with sections 10 and 11 of this policy.

12.2.1 **IAOs** are responsible for ensuring that resources are available to perform periodic information risk assessments on all information assets assigned to them on the corporate Information Asset Register (IAR). Assessments should be carried out annually or as required by the SIRO.

12.2.2 **IAOs** are also responsible for ensuring **Data Protection Impact Assessments** (DPIAs) are carried where legally required. Contact Information Governance for further information.

12.2.2 The **IAO** must designate **Deputy Information Asset Owners** and **Data Owners** roles to delegate responsibilities for information risk management and data quality standards across their directorate. These roles are in place to provide assurance and operational support to the **IAO**.

12.2.3 An information asset risk assessment template must be completed annually. The template supports IAO's, deputies, and data owners in identifying and managing information governance and data protection risks relating to their services information assets and data processing activities.

12.2.4 Where threats or vulnerabilities are identified they must be escalated to the relevant **DIAO** and **IAO**, with mitigating action plans to treat the risk. In accordance with section 10 and 11 of this policy.

12.2.5 **IAOs** must ensure that, where necessary, risks are recorded on the directorate and/ or corporate risk register ensuring that any threats or vulnerabilities are escalated with a mitigating action plan to manage the risk. For further guidance on recording risks please contact the Council's Risk Manager at riskandinsurance@lambeth.gov.uk

12.2.6 **IAOs** will ensure their Directorates complete and submit an information management self-assessment to the **SIRO** for consideration by the Information Risk Board, detailing any deviations from information security or information governance policies guidance.

12.3 If the risk is relating to the confidentiality of people's health and care information the first point of contact is the **Caldicott Guardian**.

12.4 **Information Governance** and **Information Security** provide guidance and support where service areas identify information risks. Contact details are infogov@lambeth.gov.uk and infosec@lambeth.gov.uk.

13. Confidentiality and Security

Any potential losses of information, including potential or actual security incidents or breaches, must be reported to the Data Protection Officer as soon as they are identified. The Data Breach Reporting Policy and Procedure defines the breach reporting procedure.

14. Training

14.1 All staff will undertake Information Governance and Data Protection training annually as part of LBL's annual training plan. IAOs, DIAOs and DOs are subject to additional training and guidance from Information Governance to support them in discharging their duties.

14.2 Information Security and Information Governance policies are readily available for all staff to understand their obligations in relation to information risk.

Appendix 1

EXAMPLES OF DATA BREACHES AND INFORMATION RISKS

The following examples of potential data breaches are all information risks. The categories are not mutually exclusive. A single breach can fall under one, two or all three categories.

Breach of Confidentiality:
Unauthorised or accidental disclosure of, or access to, personal data.

Examples of a Breach of Confidentiality (not exhaustive)

1. Accidentally or intentionally emailing someone's personal data to another person or by forwarding personal data in an attachment to the wrong person.
2. Sending a bulk email using 'to' or 'cc', instead of using 'bcc' (blind carbon-copy) thereby disclosing email addresses.
3. Sharing confidential information about a person with his or her family members or friends without their consent or lawful authority.
4. Sharing client's personal data with another body without permission or the lawful authority to do so.
5. Leaving personal or sensitive information accessible to others, for example on an unsecure computer or mobile device.
6. Sharing employees' personal data, like payroll details, bank details, home addresses and medical records without consent or the authority to do so.
7. Allowing others, accidentally or intentionally, to overlook or view personal data, on laptops or other mobile device, for example on public transport.

Breach of Data Integrity:
Unauthorised or accidental alteration of personal data.

Data integrity refers to the overall accuracy, completeness, and consistency of data. It includes, but is not limited to, the safety of data and security. Data integrity includes ensuring personal data is safe from any outside forces.

Examples of a Breach of Integrity (not exhaustive)

1. Human error, for example when individuals enter information incorrectly, duplicate or delete data or make mistakes during the implementation of procedures meant to safeguard information.

2. Outside parties (hackers) gaining access to systems or devices.

3. Bugs and viruses, including **s**pyware, malware, or other software gaining access that can invade systems and alter, delete, or steal data.

4. Compromised hardware, for example a sudden computer or server crash. A significant failure may be an indication that hardware has compromised. Compromised hardware may render data incorrect or incomplete, limit or eliminate access to data.

5. An office break-in where personal files are kept in unlocked storage.

6. When natural disasters strike, power goes out, or hackers disrupt database functions, where physical integrity is compromised.

Breach Data Availability:
Unauthorised or accidental loss of access to, or destruction of, personal data.

Examples of an availability breach (not an exhaustive list)

1. Unavailability of data due to a power failure.

2. Unavailability of data due to a cyberattack that prevents access to and/or destroyed records.

3. Misplacing or losing paper records where the data is not recorded elsewhere.

4. Accidently or intentionally deleting data before the retention period expires.

5. Failure to allow access to officers who lawfully require access.

6. A lost decryption key to encrypted data.

Appendix 2

NB: For full information on Lambeth Council's Risk Assessment Matrix and risk scoring you should refer to the Risk Management SharePoint site or email riskandinsurance@lambeth.gov.uk

1. London Borough of Lambeth Risk Appetite Statement

"LBL seeks to identify, assess and respond to all strategic and key operational risks that may affect the achievement of key business objectives and borough plan outcomes. When a risk has been identified and rated, LBL will adopt a risk response based on the nature of the risk"

2. Risk Assessment Matrix

Risk Appetite Process

Each time a risk is identified (whether for a project, programme, objective or outcome) the following three step process should be followed:

1. Score your risks – using the Risk Scoring Matrix.

2. Risk Category Identification and Risk Appetite threshold – using the Risk Appetite Matrix.

3. Risk Responses – using the Risk Responses table.

Step 1 Score your risks

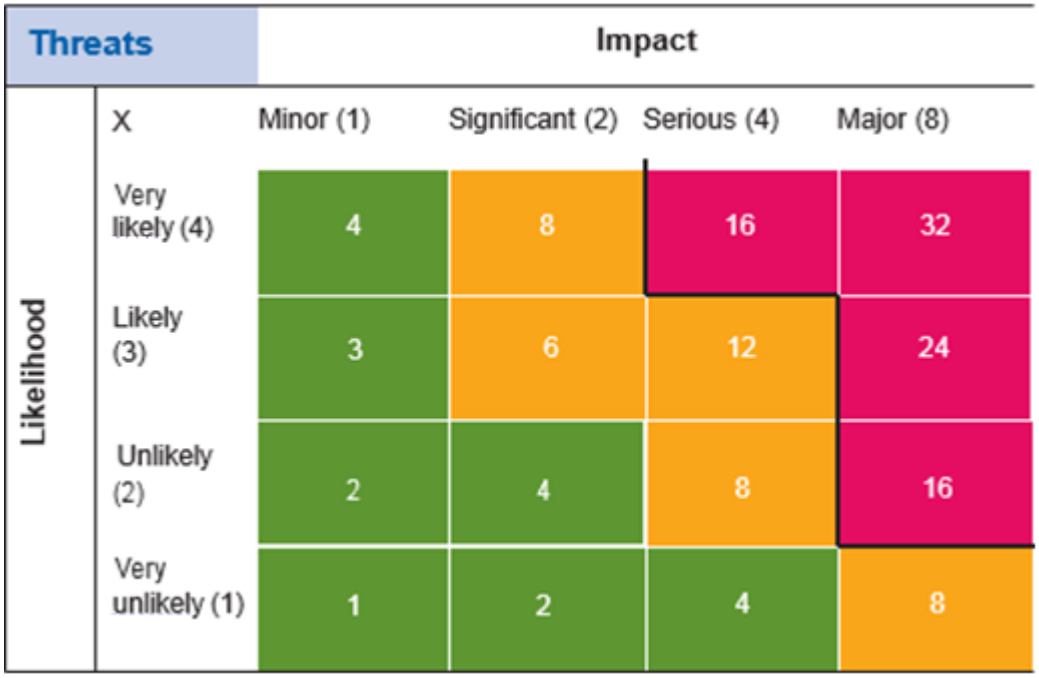
Score your risks using the Risk Scoring Matrix below. This is done by selecting the likelihood of the risk occurring and then deciding what the potential impact would be if the risk occurred. Where these two scores meet is your risk score. **NB** – When calculating current risk scores, make sure you consider all control measures/plans that you may already have in place which help to mitigate this risk. When you are choosing your Likelihood and Impact scores, make sure that you select realistic options.

Example 1:

You have a risk which you believe is Likely to happen (**score of 3**) and the Impact would be Significant (**score of 2**). This gives you a **score of 6** on the Risk Scoring Matrix.

Example 2:

You have a risk which you believe is Unlikely to happen (**score of 2**) and the Impact would be Major (**score of 8**). This gives you a **score of 16** on the Risk Scoring Matrix.


Threats
Impact
Likelihood
X
Minor (1)
Significant (2)
Serious (4)
Major (8)
Very likely (4)
4
8
16
32
Likely (3)
3
6
12
24
Unlikely (2)
2
4
8
16
Very unlikely (1)
1
2
4
8

Appendix 3.

LBL's Risk Appetite Thresholds

Risk Appetite Level	Risk Appetite Description	Risk Score
Averse	**Avoidance of risk and uncertainty is a key objective. Exceptional circumstances are required for any acceptance of risk**	**1-2**
Minimal	**Preference for the ultra-safe options that have a low degree of risk and only have a potential for limited benefit**	**3-4**
Cautious	**Preference for the safe options that have a moderate degree of risk and may only have**	**6-8**
Open	**Willing to consider all options and choose one that is most to result in successful delivery. Risk will be minimised while also providing an acceptable level of business benefit**	**12-16**
Hungry	**Eager to realise benefits and to choose options to achieve this despite the higher risk**	**24-32**

The Council's Risk Appetite or tolerance in respect of information governance is "Averse" or "Minimal" (a score of 1 to 4). Any information asset or information process with a risk score above 4 is to be subject to "risk treatment" as set out in item 11 of the Policy.

NB: for information governance a score of 14 or above should be regarded as "Hungry"