Information Governance & Risk Policy
Melton Borough Council
Document Version: V1.0
Review Date: 1 May 2019
Owner: Principal Solicitor (& Data Protection Officer)

Document History Revision Date	Version Number	Summary of Changes
20180309	V0.1	Original Draft
20180320	V1.0	Approved by SMT

1. Introduction

1.1 Information and personal data are major assets that Melton Borough Council ('the Council') has a responsibility to protect, and where required by law, to publish. They take many forms and include information and data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes, disks or other electronic media and spoken in conversation or over the telephone.

2. Aim

2.1 To provide a framework for the management of information requests made to the Council, and the management and protection of personal data held by the Council.

2.2 To assist staff to meet the presumption for disclosure of information required by legislation thereby promoting greater openness, provide increased transparency of decision making and to build public trust and confidence.

2.3 To ensure all legal obligations on the Council are met including confidentiality of information relating to such areas as personal privacy, commercial sensitivity, security issues, and where disclosure would not be in the public interest.

3. Applicability

3.1 This policy applies to all information and personal data held by the Council. Information and personal data can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Recordings.
- Photographs

4. Review and Maintenance

4.1 This policy will replace any previous Information Governance & Risk Policy, Data Protection Policy, or Freedom of Information Policy.

4.2 This policy is agreed and distributed for use across the Council by SMT. It will be reviewed tri-annually by the Principal Solicitor, who will forward any recommendations for change to the Director of Legal & Democratic Services for consideration and distribution.

5. Need for an Information Governance & Risk Policy

5.1 The information and personal data stored in the Council's manual and electronic information systems represent an extremely valuable asset on which is placed an ever-increasing reliance for the effective delivery of services. The value of and our reliance on our information makes it necessary to ensure that:

- All systems, manual or electronic, that create, store, archive or dispose of information or personal data are developed, operated, used and maintained in a safe and secure fashion.
- The public and all users of the Council's information systems are confident of the confidentiality and accuracy of the information and personal data used.
- All legislative and regulatory requirements are met.
- All transmission and essential sharing of information with partners, be that in manual or electronic format, is properly authorised and effected within agreed sharing protocols.
- An up-to-date Information Asset Register will be maintained.

6. Legal Requirements

6.1 The Council is obliged to comply with all relevant UK and EU legislation. This requirement to comply is devolved to Elected Members, who may be held personally accountable for any breaches of personal data security for which they may be held responsible.

6.2 The Council shall comply with the following legislation and other legislation and guidance as appropriate:

- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Data Protection Act 2018
- General Data Protection Regulation (Regulation EU 2016/679)
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Environmental Information Regulations 2004 (SI 2004:3391)
- Protection of Freedoms Act 2012
- Local Government Transparency Code of Practice 2015
- Freedom of Information Act 2000 Section 46 Code of Practice for Records Management

7. Policy Statement

7.1 Melton Borough Council supports the objectives of the Freedom of Information Act 2000, the Data Protection Act 2018, the General Data Protection Regulation, and other legislation relating to Data Processing and information access, including the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Environmental Information Regulations 2004 and the Protection of Freedoms Act 2012. This policy aims to assist staff with meeting their statutory and other obligations which covers the issues of Information Governance & Risk.

8. Objectives

8.1 The policy is intended to establish and maintain the security and confidentiality of personal data, and provide a framework for maintaining the normal business activities of the Council by:

- Creating and maintaining within the organisation a level of awareness of the need for Freedom of Information and Data Protection as an integral part of the day to day business;
- Ensuring that all data users are aware of and fully comply with the relevant legislation as described in policies and fully understand their own responsibilities;
- Ensuring that all information users are aware of the rights of requesters in accessing Council information under the Freedom of Information Act 2000;
- Ensuring that all data users are aware of the rights of data subjects in accessing and correcting their personal data under the Data Protection Act 2018;
- Protecting sensitive personal data from unauthorised disclosure;
- Safeguarding the accuracy of information;
- Protecting against unauthorised modification of information
- Storing, archiving and disposing of sensitive and confidential information in an appropriate manner;
- Lawful use or sharing of Council information.

8.2 The Council will achieve this by ensuring that:

- Confidentiality of personal data and exempt information is assured;
- Regulatory and legislative requirements are met;
- All transmission and essential sharing of information internally or with partners, in manual or electronic format, is properly authorised and effected within agreed sharing protocols.
- Freedom of Information and Data Protection training is provided;
- All losses of personal data, actual or suspected, are reported, investigated and any resulting necessary actions taken;
- Standards, guidance and procedures are produced to support this policy.

9. Scope

9.1 The policy applies to all:

- Information and personal data held by the Council whatever format in which it is held;
- Locations from which Council systems are accessed (including home use or other remote use). Where there are links to enable partner organisations to access Council information, prior assurance must be obtained that information security risks have been identified and suitably controlled.

10. Responsibilities

10.1 The Director of Legal & Democratic Services is the Senior Information Risk Owner (SIRO) and has overall responsibility for Information Governance & Risk within the Council.

10.2 The Principal Solicitor is responsible for:

- Undertaking the mandatory role of Data Protection Officer as defined in the General Data Protection Regulation and the relevant tasks as defined in the Regulation (**Appendix B**)
- Developing, implementing and maintaining the corporate Freedom of Information and Data Protection and relevant Information Governance & Risk policies, procedures and standards that underpin the effective and efficient creation, management, dissemination and use of personal data;
- Provision of Freedom of Information and Data Protection support and advice to staff and managers;
- The production, review and maintenance of Freedom of Information and Data Protection policies and their communication to the whole Council;
- Provision of professional guidance on all matters relating to Freedom of Information and Data Protection;
- Oversight management of all information data protection breaches and suspected breach investigations;
- Provision, via the Intranet, of Freedom of Information and Data Protection Awareness briefing materials and, through the MIKE training system, of on-line training;
- Oversight management of all information requests under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 2018, and any subsequent appeals and complaints to the Information Commissioner;
- Management and recording of information sharing processes and agreements;
- Production of an annual Information Governance & Risk Report.
- To ensure that the Council manages its records in accordance with the FOI Section 46 Code of Practice and records management requirements **(Appendix C).**

10.3 All Directors and Managers will:

- Implement this policy within their business areas;
- Ensure compliance to it by their staff;
- Support the independence of the Principal Solicitor with respect to their role as Data Protection Officer.

10.4 Additionally they will specifically ensure that:

- All current and future users of Council information are instructed in their data protection responsibilities and have access to and have read the Information Governance & Risk Policies and guidance.
- Authorised users of computer systems/media are trained in their use and comply with policy and procedural controls to protect personal data.
- Determine which individuals are given authority to access specific information systems. The level of access to specific systems which
- contain personal data should be on a job function need, irrespective of status.
- Any breach of this policy, real or suspected, is reported as required in the Information Security Incident Reporting procedure.
- Any breach investigation is undertaken as a priority and resources are committed to any investigation in order to conclude the investigation in a timely manner.

11. Freedom of Information & Environmental Information Principles

11.1 Melton Borough Council is committed to an access to information framework that ensures:

- All requests for information are dealt with promptly and within statutory timescales;
- Advice and assistance is offered to help any enquirer frame their request so that they receive the information they require;
- Requests are assessed to ensure the confidentiality of personal or commercially sensitive data is not breached, disclosure is in the public interest and provision of the information is not prejudicial to provision of essential Council Services;
- Information is withheld if a legitimate exemption applies and the application of the exemption is explained to the enquirer;
- All enquirers are kept informed in a timely manner of the progress of their request and of any delays to which it may be subject;
- A full and proper information risk management process is in place at all times;
- Assistance is offered to any enquirer to help them understand the information they receive;
- All enquirers are advised of their rights to question the information received and know what has not been provided and why;
- All enquirers are advised of their right to take any appeal or complaint to an internal review process (where appropriate) or to the Information Commissioner, if they are dissatisfied with the service received or the information provided;
- The majority of information which can be made publicly available is published on the Melton Borough Council website as and when resources allow;
- All requests are monitored and performance indicators made available to demonstrate compliance with the legislation;
- All staff are provided with suitable training, guidance and procedures to enable them to manage requests for information;
- Charges are raised in accordance with **Appendix A**. (All charges owed must be paid in advance. No work will be undertaken until the fee is paid);
- The Principal Solicitor is responsible for the management and monitoring of all requests for information made under the legislation;

- The Principal Solicitor is responsible for ensuring the access to information process is regularly audited to ensure compliance with statutory requirements, and that relevant national codes of practice are followed.

12. Processing Freedom of Information and Environmental Information Requests

12.1 All Requests for information should be sent at first instance to the Legal & Democratic Services team. These will be logged on the central logging system and acknowledged to the requester within 3 working days.

12.2 The Council recognises that environmental information should be processed under the Environmental Information Regulations 2004.

12.3 The procedure for dealing with information requests is contained in the Council's guidance on how to handle Freedom of Information requests which is available on the Council's Intranet.

12.4 Ways in which an information request can be made will be published on the Council's website.

12.5 The Legal & Democratic Services team will pass requests to the relevant Service Area to action the request after seeking clarification if necessary. If the Service Area is unable to deal with the request or requires clarification, they should revert to the Legal & Democratic Services team.

12.6 If a charge is applicable a fees notice will be issued by the Legal & Democratic Services team. Charges should be levied as in **Appendix A**.

12.7 Melton Borough Council will respond within the statutory time limit of 20 working days by making the information available to the data subject. This can be extended by another 20 working days or a reasonable time if the public interest is considered under FOI or it is a complex request under EIR.

12.8 If Melton Borough Council considers that an exemption applies and does not consider that disclosure is appropriate, the requester must also be informed of this within 20 working days of making the request, unless a valid extension has been notified to the requester within the initial 20 working days.

12.9 If an exemption is considered to apply, the decision not to disclose information should be made by the Principal Solicitor, in consultation with the Service Area, and the reasons for non-disclosure documented as part of a Public Interest Test (PIT) Panel convened by the Principal Solicitor.

12.10 Requests will be authorised by the relevant Service Director before release to the requester. Responses can be released by the Principal Solicitor or his/her delegate without a Director's authorisation if it is information not held, or is exempt under FOI Section 21 or EIR Regulation 6(1)(b) (information accessible elsewhere).

12.11 The Chief Executive and Directors will be informed of any sensitive requests by the Principal Solicitor and/or the Director of Legal & Democratic Services.

12.12 Councillors will be informed of any request relating to them by the appropriate Director, the Principal Solicitor or their delegates.

12.13 Information that is released via FOI or EIR that meets the definition of a dataset will be released wherever possible in an open data format, under an open government licence, and this dataset will be published and updated regularly on the Council's website or its open data pages where it is reasonable to do so.

13. Vexatious Requests

13.1 Before applying section 14 and deeming a request vexatious or manifestly unreasonable under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 respectively, the Principal Solicitor will consult the Monitoring Officer before making a decision.

14. Data Protection Principles

14.1 All organisations that 'process' 'personal data' are data controllers and are required to be registered with the Information Commissioner, as defined in the Digital Economy Act 2017. The Principal Solicitor will ensure that this is completed annually.

14.2 The Council will adopt a "best practice" approach at all times based on the Information Commissioner' guidelines, and, where appropriate, professional codes of practice.

14.3 Any data controller must observe the Data Protection principles which govern the manner in which data is collected, held and processed. The Council is committed to ensuring that all information held is necessary, used fairly and responsibly and in compliance with the principles as follows:

1. Processed fairly and lawfully

- Information will only be held where it is justified to do so and processing may be carried out where one of the following conditions has been met, namely where:-
- The individual has given their consent to the processing
- The processing is necessary for the performance of a contract
- The processing is required as part of a legal obligation
- The processing is necessary to protect the vital interests of an individual
- The processing is necessary in order to pursue legitimate interests
- Local Authorities have specific legal authority to use or disclose information under duties or powers given to them under statute.

2. Processed only for the specified lawful purposes and not processed in any way incompatible with those purposes

- The Council is one data controller. Personal data held by the Council can be used within the Council as permitted by the Council's Privacy Notice to carry out the functions of the Council. This however must be on a 'need to know' basis and appropriate security and access controls implemented

where necessary so only staff that need access to the personal data are allowed it.
- All requests for information from other public bodies, including the police, are to be in writing except in an emergency.
- When receiving requests for personal data, clarification must be obtained as to who the requesting party is, the reason why information is requested and if there is authority to give the personal data.
- Where consent is used as the legal basis for processing personal data, the Council will ensure that consent is unambiguous, freely given, and an affirmative action, with an audit trail to demonstrate that consent was gained. Where special category data are processed, the consent gained will be explicit consent.

3. Adequate, relevant and not excessive in relation to the purpose(s) for which personal data is processed

- Melton Borough Council will only hold the minimum personal information necessary to enable it to perform its functions.

4. Accurate and kept up-to-date

- All efforts will be made to ensure that information is periodically assessed for accuracy; and
- Is kept up to date.

5. Processed no longer than is necessary for the purpose(s)

- Information must be destroyed securely once it is no longer required, and kept in line with the Council's retention and disposal schedule.

6. Processed in accordance with the rights of the data subject

- Melton Borough Council recognises the rights given to people under the General Data Protection Regulation (Articles 12-22)
  - ✓ Right to Access
  - ✓ Right to Rectification
  - ✓ Right to Erasure
  - ✓ Right to Object
  - ✓ Right to Object to Automated Decision-making
  - ✓ Right to Restriction
  - ✓ Right to Data Portability
  - ✓ Right to Compensation

7. Protected by appropriate and organisational measures

- Melton Borough Council has systems in place to keep information secure. Staff must refer to the Information Security Policy.
- All staff must undertake the appropriate information training on the appropriate refresh cycle.

8. Transfer of personal data to non-EU member states

- Transfer of personal data to non-EU member states must show the necessary organisational and technical measures have been put in place to protect data; e.g. adequacy assessment.

15. Special category personal data (Article 9) and personal data relating to criminal convictions and offences (Article 10)

15.1 There are additional requirements placed upon the data controller where the holding of 'special category personal data' is concerned. The definition of 'special category personal data' is data in respect of: -

A. racial or ethnic origin
B. political opinion
C. religious or philosophical beliefs
D. trade union membership
E. genetic data
F. biometric data
E. physical/mental health
F. sexual life or sexual orientation

15.2 If disclosing special category personal data (even if required to do so by law) consent of the data subject must be obtained unless a specific exemption applies.

15.3 Additionally, if special category personal data is held, security measures for holding such data will need to be considerably higher than that for other service areas holding less sensitive data.

15.4 Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or where the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

16. Privacy Notices

16.1 Under the General Data Protection Regulation and the Data Protection Act 2018, data subjects have the right to know what the Council will use their personal data for. This is called a Privacy Notice. It should be added on all Council forms, including electronic forms and web-based forms,, where personal data is collected. Melton Borough Council will publish its Privacy Notices on the Council's website. The Council will make reasonable efforts to communicate Privacy Notices where necessary to service users with additional needs, e.g. but not limited to, translation services, easy read versions, given verbally, posters, leaflets, and so on.

17. Subject Access Requests – What the Data Controller has to do

17.1 Under the General Data Protection Regulation and the Data Protection Act 2018, data subjects have the right to know what information is held about them. This is known as a Subject Access Request.

17.2 All Requests for information under Subject Access should be sent at first instance, without delay, to the Legal & Democratic Service team at Melton Borough Council.

17.3 The procedures for dealing with Subject Access requests are contained in the guidance on how to handle a Subject Access Request which is available on the Council's Intranet.

17.4 Ways in which a Subject Access request can be made will be published on the Council's website.

17.5 The Principal Solicitor or their delegate will pass requests to the relevant Service Area to action the request. If the Service Area is unable to deal with the request or requires clarification, they should revert to the Principal Solicitor.

17.6 Subject Access Requests shall be free and without charge.

17.7 Where a request is repeated or manifestly excessive a reasonable fee may be charged in accordance with Section 3 of **Appendix A** to this Policy.

17.8 Where a request is repeated or manifestly excessive, an extension of 2 months can be implemented so long as the data subject is informed of this within 1 month of making the request.

17.9 Melton Borough Council will respond within the statutory time limit of 1 month by making the information available to the data subject.

17.10 Where a request is manifestly unfounded or excessive, Melton Borough Council can refuse to act on the request.

17.11 If Melton Borough Council considers that an exemption applies and does not consider that disclosure is appropriate, the data subject must also be informed of this within 1 month of making the request.

17.12 If an exemption is considered to apply, the decision not to disclose information should be made by the Principal Solicitor, in consultation with the Service Area, and the reasons for non-disclosure documented.

17.13 In considering whether to disclose information, Melton Borough Council must take care not to reveal the identity of another third party individual. Any information supplied by a third party should not usually be revealed without first seeking permission from the source.

18. Other Rights

18.1 The data subject also has a right to have inaccurate information corrected (right to rectification), restricted or erased (right to erasure). If a request to amend information is received from a data subject, the Principal Solicitor or their delegate must respond within 1 month to confirm what action has been taken. Any decision will be taken by a senior member of staff in the relevant Service Area in consultation with the Principal Solicitor and the reasons documented.

18.2 The data subject also has a right to know the process and information involved in any automated decisions regarding them. If the data subject objects to the decision made by automated decision, a further decision should be made by other means if possible. The data subject has 1 month in which to request a further decision be made by non-automated decisions and the data controller has 1 month to action.

18.3 The data subject has a right to receive data which he or she has provided to the Council with consent to automated processing, in a structured, commonly-used and machine-readable format and have the right to transmit those data to another controller (right to data portability). The Council has 1 month to action such a request.

19. Requests concerning the prevention of crime and disclosure required under a court order or an enactment

19.1 Wherever possible such requests should be submitted in writing.

19.2 Requests for information should be sent at first instance to the Legal & Democratic Services team.

19.3 Leicestershire Constabulary police officers should submit such requests on their own form, countersigned by their superior officer.

19.4 If any Melton Borough Council staff member is in doubt about releasing information for such requests in an emergency, they must contact the Legal & Democratic Services team immediately for advice.

19.5 There will be no charge for the processing of such requests.

20. Requests regarding legal proceedings or legal advice

20.1 Such requests should be submitted in writing.

20.2 Requests for such information should be sent at first instance to the Legal & Democratic Services team.

21. CCTV Requests

21.1 Requests for CCTV footage should be submitted in accordance with the Council's CCTV Protocol.

21.2 Requests for CCTV footage should be sent at first instance to the Legal & Democratic Services team.

21.3 Where a commercial company or organisation (e.g. solicitor, insurer, housing association) is acting on behalf of a requester, Melton Borough Council will charge as per the CCTV Policy.

21.4 Where an individual is making a request for CCTV footage involving their personal data, this will be free under Subject Access procedures.

22. Requests made on behalf of children

22.1 A request for information may be made by a parent, guardian or agent on behalf of another individual.

22.2 Requests made on behalf of others will be dealt with as above, however great care should be taken to verify the identity of those making the request if there is any doubt. It should be ascertained if the person making the request on behalf of the child has parental responsibility, or consent from the child (where the child is old enough).

22.3 Nothing is to be disclosed to a third party which would not be in any child's best interests to do so. This includes where information is requested on the child's behalf by any parent or guardian. The decision as to what not to disclose should be made by the Principal Solicitor in consultation with the relevant Service Area and the reasons for any non-disclosure documented.

23. Requests made by children

23.1 Requests by children can be made to a number of services. Any child may be allowed to see their own records unless it is obvious that they do not understand what they are asking for (Gillick Competency).

23.2 The Principal Solicitor should consider that nothing be disclosed to a child which would be likely to cause serious harm to their physical or mental health. The decision as to what not to disclose should be made by the Principal Solicitor in consultation with the Service Area and the reasons for any non-disclosure documented.

23.3 In addition, the usual principles of subject access requests as outlined in this policy will apply.

23.4 If the Council provides an Information Society Service directly to a child, the Council will take reasonable steps to verify the consent of the parent or guardian of the child if the child is under the age of 13 years.

24. Disclosure to a Third Party

24.1 Any request for data received from a third party should be in writing and the third party must be identified. Where the third party seeks to rely on a legal authority for disclosure, they must quote the relevant authority and provide evidence.

24.2 Unless an exemption applies (see below), personal data will not usually be disclosed, except where the data subject consents to such disclosure.

24.3 'Third party' includes members of a data subject's family, legal representatives of a data subject , a data subject's employer and any organisations acting on behalf of an individual such as the Citizen's Advice Bureau or a Housing Association.

24.4 Requests for access from a third party should be accompanied by either an Authority to Disclose from the data subject or in the absence of this, necessary

enquiries should be undertaken by the Principal Solicitor to ascertain if consent is given. If there is any doubt, written confirmation direct from the Data Subject should be sought.

24.5 The 1 month time limit also applies to requests for data from a third party, including the requirement to inform why a decision for not disclosing is made and the reasons for doing so. Again, this decision should be taken by a senior member of staff and the reasons for not disclosing documented and made clear to the third party.

24.6 Nothing should be disclosed which would be likely to cause serious harm to a child's or vulnerable adult's physical or mental health. In all requests for access, the interests of the subject, particularly in the case of a child or vulnerable adult must be paramount and the duty of the Council to protect children and vulnerable adults from potential harm of primary importance.

24.7 Requests received from third parties relating to deceased individuals will be handled in line with guidance published by the Information Commissioner's Office.

25. Exemptions

25.1 The rights of data subjects are subject to certain statutory exemptions. The Council will disclose personal information, without the data subject's consent in accordance with the Data Protection Act 2018. This includes but is not limited to:

- On production of a court order for disclosure
- Where the purpose of disclosure is to enable the Authority to assess or collect any tax or duty or any imposition of a similar nature
- Where the purpose of disclosure would be to prevent or detect a crime, apprehend or prosecute offenders
- By order of the Secretary of State
- Where we are obliged by any law to disclose information
- Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject
- Where disclosure would be to safeguard national security
- To Melton Borough Council councillors, where disclosure is necessary to enable them to fulfil their statutory duties as Councillor, in accordance with the Elected Members Access to Information Regulations.

26. Other Rights of the Individual

26.1 This policy shall not affect or in any way compromise an individual's rights under the Human Rights Act 1998.

26.2 At present an individual's right to privacy outweighs another individual's right to information under the Freedom of Information Act (i.e. if personal data is contained in a document that document cannot usually be released to a third party).

27. Information Security

27.1 Personal data will only be kept for as long as the service provided to the data subject is in existence or is as required by law. If there is no legal requirement to keep the records, they will be destroyed as soon as is practicable in line with Melton Borough Council's Retention and Deletion Schedule.

27.2 Personal data should be handled in accordance with the Council's Information Security Policies.

27.3 In the event that employees take home manual or computerised files containing data, it is the employee's responsibility to ensure that such data is made secure.

27.4 Any data protection breach must be reported immediately to a manager as required in the Parkside Information Security Incident Reporting procedure.

27.5 All personal data breaches must be reported to the ICO within 72 hours (unless there is reasoned justification) by the Data Protection Officer unless it is unlikely to result in a risk to the rights and freedoms of the data subject.

27.6 Managers must submit a Data Protection Impact Assessment (DPIA) to the Legal & Democratic Services team for all new projects, procurement, commissioning or services that they undertake at the start of any such proceeding.

27.7 The Data Protection Officer will assess any final DPIA submission and if they consider that it meets the necessary Article 35 and Article 36 criteria, will submit the DPIA to the ICO for consultation as per the ICO's guidance.

28. Elected Members

28.1 Councillors must ensure that Data Protection legislation and policies are complied with whatever role they may exercise. If the Member is in any doubt, they should contact the Principal Solicitor for clarification.

28.2 If a Councillor seeks clarification over whether they are processing data as a separate data controller from Melton Borough Council, information for Councillors is also available from the Information Commissioner's website at https://ico.org.uk/

28.3 If the Councillor is processing data for their own purposes they must register with the Information Commission as a data controller as well as ensure compliance with the principles of the Data Protection Act 2018. The Principal Solicitor will complete the annual registration on the behalf of each elected member.

29. Information Sharing

29.1 The Council will require its partners and agents through contractual terms, partnership agreements and information sharing agreements to comply with the law when providing services to the Council and when sharing data with the Council.

29.2 Managers responsible for procurement of services must ensure that data protection impact assessments are carried out, potential bidders are compliant with data protection requirements and the necessary Data Processing Agreements are put in place when contracts are awarded.

29.3 Managers responsible for services which share personal data with outside partners and agencies on a regular, organized basis must ensure that a written Information Sharing Agreement is in place.

29.4 The Information Sharing Agreement must be agreed by the Principal Solicitor, who will record a copy centrally for monitoring purposes.

29.5 The Information Sharing Agreement must be signed by the relevant Service Director for single service agreements and the Director of Legal & Democratic Services for cross-service agreements.

30. Use of Personal Data in Marketing

30.1 Melton Borough Council will comply with the Privacy and Electronic Communications Regulations (PECR).

30.2 Personal Data collected by Melton Borough Council will only be used for marketing purposes where customers have been told this will happen via a Privacy Notice as part of a soft opt-in during a sale or negotiation of a sale, or where customers have explicitly opted-in (consented) to receive such information.

30.3 All emails sent to customers for marketing purposes will include a 'how to opt-out' message.

30.4 Databases used by Melton Borough Council for marketing purposes will be 'cleansed' at least every two years to determine customers still wish to receive marketing information and to verify the accuracy of the data.

31. Compliance with the Legislation

31.1 The Council recognises the need to make the contents of this Policy known and ensure compliance by every employee.

31.2 All staff will be mandatorily trained in basic Freedom of Information and Data Protection principles and made aware of this policy and of relevant Melton Borough Council guidance which is available. Freedom of Information and Data Protection awareness will be included in the corporate induction course and training updates for staff will also be provided biannually. The Principal Solicitor will notify staff of changes to Freedom of Information and Data Protection legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

31.3 All Councillors will be offered training in Freedom of Information and Data Protection where possible.

31.4 The Council also recognises the need to make its policies known and accessible to the public. This policy will be published on the Council's website.

31.5 The Council must notify the Information Commissioner's Office annually regarding what personal data it intends to process. An internal review of these notification requirements will be undertaken by the Principal Solicitor annually and as required by the needs of the Council. The Information Commissioner will be informed of any changes required to the notification.

31.6 Melton Borough Council expects all employees to comply fully with this policy, the Freedom of Information and Data Protection principles, other information legislation and the Council's procedures. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following from this policy.

31.7 Individual employees are affected in the same way as the Council as a whole. Anyone contravening the Freedom of Information Act 2000 and/or Data Protection Act 2018 could be held personally liable and face court proceedings for certain offences which may result in a fine and/or a criminal record.

31.8 The Principal Solicitor can recommend service areas, which are causing concern over Freedom of Information and/or Data Protection compliance, to Internal Audit for further investigation.

32. Complaints

32.1 Complaints relating to any information access request or data protection matter should be made in writing and addressed to:

The Principal Solicitor & Data Protection Officer
Melton Borough Council
Parkside
Station Approach
Burton Street
Melton Mowbray
Leicestershire
LE13 1GH

34.2 If the applicant is still unhappy following the appeal decision they should be advised to write to:
The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
www.ico.org.uk

Appendix A

Applicable Fees

1. Freedom of Information Act 2000

1.1 The Council will not charge for answering any request for information made under the legislation except that the Council may charge for the cost of disbursements in the production of material in respect of complying with an information request.

1.2 The Council will not provide information where the cost of compliance exceeds the statutory limit. The Council will seek to work reasonably with requesters where there is a risk of requests breaching the statutory limit.

1.3 Where a fee is to be charged a fee estimate will be provided to the requester.

1.4 The Authority will not take into account any cost other than those set out in the Fees Regulations (SI 2004/3244 Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations). In particular, it will not take into account:

- Time taken to check a request meets the Act's requirements;
- Considering if the requested information should be withheld because of an exemption;
- Considering whether a request is vexatious or repeated;
- Obtaining authorisation to send out the information;
- The time taken to calculate any fee charged, including any costs associated with producing and serving a fees notice; or
- Providing advice and assistance under the Act.

1.5 The applicant will be sent a fees notice detailing the estimated costs of meeting the request as soon as possible, but within 20 working days of receiving the request. The 20 working days clock will stop ticking when the fees notice is issued and restart when payment is received - if a cheque this means when that has cleared.

1.6 No further work need be undertaken until full payment has been received. On receipt a cheque must be passed immediately to Financial Services for clearance. Unless advised to the contrary the co-ordinating officer should assume the cheque is cleared after four working days.

1.7 If full payment is not received within three months of the date that the fees notice is issued the request should be closed. Any subsequent request should be treated as a new request.

1.8 If the cost of finding the requested information is:

(i) *Below the prescribed limit*: The only charge will be for the Disbursements (see below for relevant charges) involved in answering the request. No charge can be made for staff time taken in finding or supplying the information.

(ii) *Over the prescribed limit*: Any request that will cost more than prescribed limit will be refused as allowed by legislation. The Council will work with requesters in these cases to reduce costs, but will not undertake any work where the prescribed limit ceiling is breached.

(iii) *Working out the prescribed limit*: This is an estimate of the staff time needed to do any or all of the following when answering the request and includes:

- Determining if the Authority holds the requested information;
- Locating the information or a document that contains the information;
- Retrieving the information or a document that contains the information; and
- Extracting the information from a document containing it.

1.7 Disbursements costs are incurred in:

- Complying with the request for information in a specific format (e.g. summary, inspection, etc.);
- Reproducing any document; and
- Postage and other forms of transmission e.g. fax.

Charge rates are:

DISBURSEMENT CHARGE

- Complying with any obligation under the Act when communicating the information, for example putting the information in a specific format - Charged at cost.
- Time spent putting the information in the requested format, summarising the information or supervising an inspection of the information is charged at £25 an hour.
- Photo-copying - 20p per A4 single side. Staff time involved is not chargeable.
- Postage and other forms of transmission e.g. fax, CD, DVD - Charged at cost. Staff time involved is not chargeable.

1.8 Where the applicant asks to see the information, but does not want a copy of it no charge will be made. The applicant must <u>not</u> be left alone with the information. Staff charges for accompanying the applicant while the information is inspected will be charged at £25 an hour under Freedom of Information legislation. Environmental information can be viewed free of charge where possible.

1.9 The costs of answering more than one request can be added together (or aggregated) for the purpose of estimating if the threshold will be exceeded where they:

- Are either from the same person or from different persons who appear to be acting in concert or in pursuance of a campaign; and
- Relate to the same or similar information; and
- Have been received within a space of 60 consecutive working days.

1.10 Each request will be charged at the average of the costs for answering all requests. In case where a request has been made and paid for and subsequent requests are made then costs will not be so averaged.

1.11 All applicable charges to access information should be included in the Publication Scheme ('The Scheme') as published on the Council's website. This will be:

- As defined by legislation; or
- At cost.

1.12 Where applicable, legislative charges will take precedence followed by existing charging practice. Any requested information that is not in the Scheme will be included in the Scheme at the next review. Any relevant charges will be identified n the Scheme at this point.

1.13 The Copyright, Designs and Patents Act 1988 allows copyright information to be reused without the user obtaining formal consent from the copyright holder for:
- Research for non-commercial purposes;
- Private study; or
- News reporting and review

1.15 Data available through the Freedom of Information Act 2000, Transparency Agenda and Protection of Freedoms Act 2012 which is available on the Council's website can be downloaded and re-used in line with conditions laid out in the Open Government Licence.

2. Environmental Information Regulations 2004 Charges

2.1 All requests will be charged as for the Freedom of Information Act and with regard to applicable case law.

3. Data Protection Act Charges

3.1 All Subject Access Requests will be free of charge as required by the Data Protection Act 2018 and the General Data Protection Regulation. Where a request is repeated or manifestly excessive a reasonable fee may be charged.

3.2 Requests for CCTV footage will be charged for as per the CCTV Protocol..

4. Value Added Tax

4.1 If the requested information is available from another non-Public Authority source then Value Added Tax is chargeable. In all other cases Value Added Tax is not chargeable.

5. Mixed Requests

5.1 Requests may be made for access to information under more than one of the above pieces of legislation. Charges will be raised as applicable for each applicable piece of legislation.

6. Information supplied under other legislation

6.1 Requests for information under other legislation, where there is no legal prohibition on charging, will be charged for at £25 per hour.

Appendix B

Tasks of the Data Protection Officer

1. The Data Protection Officer's tasks are:

   (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

   (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

   (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 (DPIAs);

   (d) to co-operate with the supervisory authority;

   (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 (DPIAs), and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

3. In addition the Data Protection Officer must carry out the following tasks in service areas with law enforcement roles:

   (a) assigning responsibilities under those policies,

   (b) raising awareness of those policies,

   (c) training staff involved in processing operations, and

   (d) conducting audits required under those policies.

Appendix C

Records Management

1. Introduction

1.1 Records management in local government is regulated by the FOIA 2000 Section 46 Code of Practice. The Code of Practice Part 1 specifically covers records management and sets out the key elements of good practice. To meet these, a local authority should:

- have in place organisational arrangements that support records management – this includes the recognition of records management as a core corporate function, the allocation of clearly defined roles and responsibilities, and the provision of appropriate training;
- have in place a records management policy covering information security, records retention, destruction and archive policies, and data protection (including data sharing) policies;
- retain the records needed for business, regulatory, legal and accountability purposes;
- have in place systems that enable records to be stored and retrieved as necessary;
- know what records are held, where they are and ensure that they remain useable;
- ensure that records are stored securely and that access to them is controlled;
- define how long records should be kept for, and dispose of them when no longer needed;
- ensure that records shared with other bodies or held on their behalf are managed in accordance with the code; and
- monitor compliance with the code.

1.2 Following the Code of Practice will help the local authority with:

- The FOI Publication Scheme
- What information falls under the Public Sector Information (PSI) Regulations
- The Retention and Disposal schedule
- The Information Asset Register

- The ICO Documentation of Processing requirements

- Compliance with the requirements of data protection, in ensuring that information is not kept for longer than is necessary for the purposes for which it was collected and held

- The inventory of documents stored at the Council's Repository

2. Responsibilities

2.1 The responsibility for records management at Melton Borough Council will sit with the Director of Legal & Democratic Services and such persons in their service as they direct to discharge records management duties, and in conjunction with the Directors of the other services and their staff, as the owners of the Council's information assets

2.2 The Council's Information Management Group (IMG), chaired by the Director of Legal & Democratic Services, as Monitoring Officer, will constitute the internal forum for the co-ordination of such activities.

2.3 Individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the authority's record management guidelines.

3. Scope

3.1 Records management applies to the whole Council. This means all records created, received or maintained by staff of the authority in the course of carrying out their corporate functions.

3.2 Records are defined as all those documents which facilitate the business carried out by the authority and which are thereafter retained (for an appropriate period in accordance with the lawful retention and disposal schedule) to provide evidence of its transactions or activities.

3.3 Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

3.4 There will be annual reviews of stored information, and revisions where necessary, as required by audit. Currently these reviews take place in November each year.

3.5 A proportion of the authority's records will be selected for permanent preservation as an enduring record of the conduct of its business, in accordance with the lawful retention and disposal schedule, and for historical research. Arrangements may be entered into with the County Record Office to facilitate this process.

3.6 The transfer of records to archives is covered by Part 2 of the Section 46 Code of Practice.

4. Retention and disposal

4.1 Hitherto, the Council has used guidance, in the form of the Records Management Society of Great Britain's Guidance, and the Council's supplementary matrix, which are available on the Council's shared drive, under 16 Information Management\Access to Information\DP,FOI & EIR, PSI\General Guidance Notes.

4.2 All records are to be kept for the minimum periods listed in the guidance unless subject to litigation. Please seek legal advice if unsure.

4.3 With the introduction of GDPR, the Council will aim to use the latest retention and disposal guidance supplied by the Local Government Association via the LG Inform Plus system.

4.4 The Council's Clear Desk Policy contains guidance on the confidential disposal of documentary materials.

5. Security and access

5.1 An authority should ensure that its arrangements for storage, handling, and transmission of records reflect accepted standards and good practice in information security. The Council's Information Security policies and procedures will be applied, and should be kept up-to-date.

5.2 The Council should ensure that internal access to information is appropriately restricted, particularly with reference to personal data or confidential information. This will include the use of electronic restrictions in the form of passwords, menu access security set-up, and encryption. These measures will be subject to audit.

5.3 The Director of Legal & Democratic Services should ensure that the Council's Protective Marking Policy is up-to-date and properly applied.