Information Assurance Policies and Guidance

Information Governance & Risk Policy

Document Version: v2.3
Review Date: 01 September 2020

Owner: Head of Information Governance & Risk

Document History

Revision Date	Version Number	Summary of Changes
01012013	V0.1	Original draft
04012013	V0.2	Amendments suggested by Head of Information Assurance.
09012013	V0.3	Amendments suggested by Director of Information & Customer Access.
14032014	V0.4	Update to procedure for sensitive requests, addition of Protection of Freedoms Act datasets requirements, addition of Caldicott Guardian log to meet IG toolkit requirements, addition of traded service, addition of charges.
10042015	V0.5	Update contact details, plus release arrangements for information not held and s21
200516	V0.6	Update contact details and job titles, remove references to e-handbook, Information Risk Manager, Head of Information Assurance and IMPB, add delegates to Head of IG & Risk where applicable. Add referral of vexatious requests to City Barrister. Update open government licence information, & revise acknowledgement days from 2 to 3.
300517	V0.7	Amendments to Sections 1-text, 6-addition of AHRA & Transparency Code, 11-addition of EIR elements, 12-text, 13-addition of manifestly unreasonable (EIR) category,14-text, 16- Rename FPN as Privacy Notice,19-Amendments to Section 29 & 35 requirements, 20-text & revised s35 charge, 24-requests for deceased records added, 27-Caldicott amended-meetings and incidents, 28-text, 30-amendments re information sharing, rename PIAs to DPIAs, 31-addition of opt-in aspects and Appendix B; regarding deceased records and charging.
281217	V2.0	Updated to reflect changes required by GDPR / Data Protection Act 2018
060618	V2.1	Updated to reflect new clause numbering required by Data Protection Act 2018 plus requirement for a policy on law enforcement data processing activities.

110918	V2.2	Updated to reflect inclusion of volunteers, some exemptions from publication on FOI disclosure log and rename IG toolkit to Data Protection & Security Toolkit, plus formatting.
171019	V2.3	Updated, minor amendments to text; and • 3.1 Applicability amended • 7.1 Inclusion of RoPSI • 7.2 Refer to the Additional Policy Document • 8.1 Inclusion of EIR • 10.2 Updated reference to DPA 2018 • 12.3 Inclusion of reference to statutory codes of practice for FOIA & EIR • 12.6 Amended costs refusal • 14.1 Reference to DPA 2018 Charging regulations • 14.3 Amendment to legitimate interests reference • 14.4 Right to be Informed added • 16.3 Privacy Notice updates • 16.4 Staff Privacy Notice • 17.6 Charging for SAR • 19.3 Removed reference to “Leicestershire” • 21.3 Linked to Charging reference at 20.3 • 28.5 Added “High Risk” • 29.3 No registration required for elected members • Appx B 7.1 Updated charges for deceased records

1. Introduction

1.1 Information and personal data are major assets that Leicester City 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 footage.
- Recordings.
- Photographs

4. Review and Maintenance

4.1 This policy will replace any previous Information Governance & Risk Policy.

4.2 This policy is agreed and distributed for use across the Council by CMT. It will be reviewed annually by the Head of Information Governance & Risk, who will forward any recommendations for change to the City Barrister and Head of Standards 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. An up to date Information Asset Register will be maintained.
- 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.

6. Legal Requirements

6.1 The Council is obliged to comply with all relevant UK and EU legislation. This requirement to comply is also 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 as appropriate:

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

7. Policy Statement

7.1 Leicester City Council supports the objectives of the Freedom of Information Act 2000, the Data Protection Act 2018 and other legislation relating to Data Processing and information access, including the General Data Protection Regulation, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Environmental Information Regulations 2004, the Reuse of Public Sector Information Regulations 2015, and the Protection of Freedoms Act 2012. This policy aims to assist staff, contractors, students and volunteers with meeting their statutory and other obligations which covers the issues of Information Governance & Risk.

7.2 In addition, the Council will have an Appropriate Policy Document (APD) in place when carrying out sensitive processing for law enforcement purposes, the processing of criminal data and for the processing of Special Category Data as required by Paragraph1 of Schedule 1 of the Data Protection Act 2018.

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 & Environmental Information Regulations 2004;

- 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
- All staff, agency workers, contractors, students and volunteers processing Leicester city Council's data.

10. Responsibilities

10.1 The Chief Operating Officer, on behalf of the City Mayor, is the Senior Information Risk Owner (SIRO) and has overall responsibility for Information Governance & Risk within the Council.

10.2 The Head of Information Governance & Risk is responsible for:

- Undertaking the mandatory role of Data Protection Officer as defined in the General Data Protection Regulation and the relevant tasks defined within the Regulation (Appendix A)
- 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, Environmental 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 Learning Pool or a similar online training module, 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.

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 post holder.

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 Leicester City 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 Leicester City 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 B. (All charges owed must be paid in advance. No work will be undertaken until the fee is paid);
- The Head of Information Governance & Risk is responsible for the management and monitoring of all requests for information made
  under the legislation;
- The Head of Information Governance & Risk 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 Information Governance & Risk Team, Tel. 0116 4541300, Email: info.requests@leicester.gov.uk and these will be logged on the central IG & R 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 in line with the requirements of the Statutory Code of Practice issued under Section 45 of the Freedom of Information Act 2000; and it's equivalent code issued under Regulation 16 of the Environmental Information Regulations is contained in the Leicester City Council publication – '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 Information Governance & Risk 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 Information Governance & Risk Team.

12.6 If a charge is applicable the Council may refuse the request in its entirety or issue a fees notice will be issued by the Information Governance & Risk Team. Charges should be levied as in Appendix B.

12.7 Leicester City Council will respond within the statutory time limit of 20 working days by making the information available to the requester. 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 Leicester City 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 Head of Information Governance & Risk, in consultation with the Service Area, and the reasons for non-disclosure documented.

12.10 Requests will be authorised by the relevant Service Director, after consultation with the relevant elected member where required, before release to the requester. Responses can be released by the Head of Information Governance & Risk 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 Operating Officer, City Mayor, Deputy Mayors and Directors will be informed of sensitive requests by the Information Governance & Risk Team weekly.

12.12 Councillors will be informed of any request relating to them by the appropriate Director, The Head of Information Governance & Risk or her 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 open data pages where it is reasonable to do so.

12.14 Responses to FoI requests will normally be published in a reasonable time on the Council's FoI disclosure log unless a relevant exemption applies to the request as well as the response.

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 Head of Information Governance & Risk 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 Data Protection (Charges and Information) Regulations 2018. The Head of Information Governance & Risk 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:-

  (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

  (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

  (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

  (d) Vital interests: the processing is necessary to protect someone's life.

  (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

  (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Note: this may only be used in limited circumstances by the Council.

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 consent was gained. Where special category data is 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

- Leicester City 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. Protected by appropriate and organisational measures

- Leicester City Council has systems in place to keep information secure. Staff must refer to the relevant Information Security Policies.
- All staff must undergo mandatory bi-annual data protection training, with staff in Adult Social Care and Public Health also to undertake training as per the requirements of NHS Digital's Data Protection & Security Toolkit.

14.4 In addition data will be processed in accordance with the rights of the data subject under the General Data Protection Regulation (Articles 12-22), namely:

- Right to be Informed
- 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

14.5 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

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 the following data: -

A. racial or ethnic origin
B. political opinion
C. religious belief
D. union membership
E. physical/mental health
F. sexual life
I. biometric (for ID purposes)
J. genetic

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.

16. Privacy Notices

16.1 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 e-forms, where personal data is collected, or on the Council's web-based forms (e-forms). Leicester City Council will publish its Privacy Notices on the Council 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 etc.

16.2 The Council will promote links to partners' Privacy Notices on its website where appropriate e.g. National Fraud Initiative, National Data Opt-Out.

16.3 The corporate Privacy Notice will be updated regularly in the light of updates to the Information Asset Register and Records of Processing Activities.

16.4 The Staff Privacy Notice will be available to staff via the intranet.

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

17.1 Under the Data Protection Act 2018 / General Data Protection Regulation, 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 Information Governance & Risk Team, Tel. 0116 4541300, Email: info-requests@leicester.gov.uk.

17.3 The procedures for dealing with Subject Access requests is contained in the Leicester City Council publication – 'Guidance on how to handle a Subject Access Request' which is available on the Council's Intranet or by request.

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

17.5 The Head of Information Governance & Risk or his/her 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 Head of Information Governance & Risk.

17.6 There is no charge for Subject Access Requests; however

17.6 Where a request is repeated or manifestly excessive a reasonable fee may be charged in line with part 3 of Appendix B of this policy

17.7 Where a request is repeated or manifestly unfounded or excessive an extension of 2 months can be implemented as long as the data subject is informed of this within one month of making the request.

17.8 Leicester City Council will respond within the statutory time limit by making the information available to the data subject.

17.9 Where a request is manifestly unfounded or excessive the Council can refuse to act on the request.

17.10 If Leicester City Council considers that an exemption applies and does not consider that disclosure is appropriate, the data subject must also be informed of this within the relevant timeframe.

17.11 If an exemption is considered to apply, the decision not to disclose information should be made by the Head of Information Governance & Risk or her delegates, in consultation with the Service Area, and the reasons for non-disclosure documented.

17.12 In considering whether to disclose information, Leicester City 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 unless it is unreasonable to do so.

18. Other Rights

18.1 The data subject also has a right to have inaccurate information corrected (rectification), restricted or erased (right to erasure). If a request to amend information is received from a data subject, the Head of Information Governance & Risk or his/her delegate must respond within one 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 Head of Information Governance & Risk 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 one month in which to request a further decision be made by non-automated decisions and the data controller has one 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 or under contract, that has undergone automated processing, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller (Data Portability). The Council has one month to action such a request.

18.4 The data subject has a right to opt out of their Confidential Patient Information being used for secondary purposes under the National Data Opt-Out Scheme unless an exemption applies. Requests for Opt-Out should be sent at first instance to the Information Governance & Risk Team.

19. Requests for 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 Information Governance & Risk Team.

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

19.4 If any Leicester City Council staff member is in doubt about releasing information under such requests in an emergency, they must contact the Information Governance & Risk Team immediately for advice.

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

20. Requests for 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 Information Governance & Risk Team.

20.3 Where a commercial company is acting on behalf of a requester, Leicester City Council will charge a non-refundable administration fee of £80.00 per request.

20.4 Where an individual is making such a request, a non-refundable administration fee of £80.00 will be charged.

21. CCTV Requests

21.1 Requests for CCTV footage should be submitted in writing.

21.2 Requests for CCTV footage should be sent at first instance to the Information Governance & Risk Team.

21.3 Where a commercial company or organisation (e.g. solicitor, insurer, housing association) is acting on behalf of a requester, Leicester City Council will charge as per 20.3 above and as required by the Council's CCTV Charging Policy.

21.4 Where an individual is making a request for CCTV footage involving their personal data, there will be no charge under Subject Access procedures in paragraph 17 above.

21.5 Leicester City Council will charge a non-refundable administration fee of £80 for CCTV footage requested for legal proceedings or legal advice.

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 Head of

Information Governance & Risk & Risk in consultation with the relevant Service Area and the reasons for any non-disclosure documented.

23. 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 Head of Information Governance & Risk 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 Head of Information Governance & Risk in consultation with the Service Area and the reasons for any non- disclosure documented.

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

23.5 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 Head of Information Governance & Risk to ascertain if consent is given. If there is any doubt, written confirmation direct from the Data Subject should be sought.

24.5 The one-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 on the Information Governance & Risk pages on the Council intranet

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 GDPR/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 Leicester City Council councillors, where disclosure is necessary to enable them to fulfil their statutory duties as councillor, as per 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 usually 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. Caldicott

27.1 This policy should be read alongside the latest Caldicott review outcomes. The Caldicott principles and processes, issued by the Department of Health, provide a framework of quality and Data standards for the management of confidential information within Health and Social Care services.

27.2 The Caldicott requirements provide a set of good practice guidelines to assist in the implementation of the GDPR/ Data Protection Act 2018 and underpin appropriate information sharing. However, it is the GDPR/Data Protection Act 2018 that is the key legislation covering all aspects of information processing, and therefore takes precedence.

27.3 Health Records should be accessed under the Access to Health Records Act 1990 and the appropriate charges applied. The relevant health professional must be consulted prior to release.

27.4 The Council will publish the name of its Caldicott Guardian on the Council's website.

27.5 A central list of Caldicott incidents will be logged as part of the Council's register of information security incidents, and The Caldicott Guardian will assess these incidents and relevant issues with the Head of Information Governance & Risk or his/her delegate at regular meetings.

27.6 The Council will be compliant with the National Data Opt-Out from March 2020.

27.7 The Council will carry out a Data Protection Impact Assessment on any data processing that is in scope of the National Data Opt-Out.

28. Information Security

28.1 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 Leicester City Council's Retention and Deletion Schedule.

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

28.3 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.

28.4 Any data protection breach must be reported immediately to a

manager as required in the Information Security Incident Reporting procedure.

28.5 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(s).

28.6 Managers must submit a Data Protection Impact Assessment (DPIA) to the Information Governance & Risk Team for all new projects, procurement, commissioning or services they undertake at the start of any such proceeding.

28.7 The Data Protection Officer will assess any final DPIA submission and if he or she feels it meets the necessary ICO criteria, will submit the DPIA to the ICO for consultation as per the ICO's guidance.

29. Elected Members

29.1 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 Head of Information Governance & Risk for clarification.

29.2 If a Councillor is processing data for the purpose of representing constituents in their ward, they are a data controller in their own right.

29.3 If the Councillor is processing data for their own purposes as per s29.2, they no longer need to register with the Information Commission as a data controller but must ensure compliance with the principles of the GDPR/Data Protection Act 2018.

30. Information Sharing

30.1 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.

30.2 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.

30.3 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.

30.4 The Information Sharing Agreement must be agreed by the Head of Information Governance & Risk, who will record a copy centrally for monitoring purposes.

30.5 The Information Sharing Agreement must be signed by the relevant Service Director for single service agreements and the Chief Operating Officer for cross service agreements. A list of such agreements will be published on the Council's web site.

31. Use of Personal Data in Marketing

31.1 Leicester City Council will comply with the Privacy and Electronic Communications Regulations (PECR).

31.2 Personal Data collected by Leicester City 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.

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

31.4 Databases used by Leicester City 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.

32. Schools

32.1 Local Authority Schools are separate data controllers and responsible for their own Freedom of Information and Data Protection policies and procedures.

32.2 Where the Council and schools need to share information and can legally do so, appropriate information sharing agreements should be implemented where necessary.

32.3 If a Subject Access request is received by a school or the Council by a member of school staff asking for information which may be held by both organisations, the Council and school should advise the requester that he or she must submit two separate requests to both organisations. The Council and school should then liaise as normal with each other as interested third parties if applicable before any disclosure is made.

32.4 If a Freedom of Information request is received by the Council but the school holds the information, the request must be forwarded to the school and/or the requester advised of this.

32.4 Requests for educational records should be processed under The Education (Pupil Information) (England) Regulations 2005 and the relevant charges applied.

32.5 Where schools require advice on Information Governance & Risk matters from the Local Authority, they should access this support via the Council's Legal Services traded service arrangements.

33. Compliance with the Legislation

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

33.2 All staff will be mandatorily trained in basic Freedom of Information and Data Protection principles and made aware of this policy and of relevant Leicester City Council publications which are available. Freedom of Information and Data Protection awareness will be included in the induction process. Mandatory training updates for staff will also be provided bi-annually. The Head of Information Governance & Risk 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.

33.3 All Councillors will be offered training in Freedom of Information and Data Protection upon election and bi-annually.

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

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

33.6 Leicester City 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.

33.7 Individual employees are affected in the same way as the Council as a whole. Anyone contravening the Freedom of Information Act 2000 and/or GDPR/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.

33.8 The Head of Information Governance & Risk can recommend service areas, which are causing concern over Freedom of Information and/or Data Protection compliance, to Internal Audit for further investigation or undertake his or her own audit, particularly in law enforcement service areas.

33.9 As well as the annual Information Governance & Risk report, The Head of Information Governance & Risk will provide weekly management data reports showing compliance with Freedom of Information requests, Subject Access requests and other data protection requests, and monthly reports on personal data breaches.

34. Complaints

34.1 Complaints relating to any information access request, National Data Opt-Out or data protection matter should be made in writing and addressed to:

Head of Information Governance & Risk &
Data Protection Officer
Legal, Coronial & Registrars Services
4th Floor, Rutland Wing
City Hall

Charles Street
Leicester
LE1 1FZ
info.requests@leicester.gov.uk, or,
data-protection-officer@leicester.gov.uk

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

Task of the Data Protection Officer

- 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

- 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

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

- to cooperate with the supervisory authority

- 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.

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.

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 B

Applicable Fees

1. Freedom of Information Act 2000

1.1 The Council will charge for answering any request for information made under the legislation except that no charge will be made for a value of less than £5.75. All charges will be communicated in writing to the applicant through a fees' notice.

1.2 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.

1.3 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.

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

1.5 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.

1.6 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	10p per impression, regardless of size. 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 not 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 included in the Publication Scheme must be included in the Scheme e.g. 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 in 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 with the exception that full charges will be made at all times when the initial £5.75 trading limit is breached.

3. Data Protection Act Charges

3.1 All Subject Access Requests and other data subject rights requests will be free of charge. Where a request is repeated, or manifestly unfounded or excessive a reasonable fee may be charged based on the administrative costs of complying with the request.

3.2 Requests for Educational Records will be charged as per the Education (Pupil Information)(England) Regulations 2005. This is normally the cost of supplying the information.

3.3 Requests submitted under the Data Protection Act 2018 Schedule 2 Part 1(5) (Legal Proceedings and Advice) will be charged as follows:

- Where a commercial company is acting on behalf of a requester, Leicester City Council will charge a non-refundable administration fee of £80 per request.
- Where an individual is making a request, a non-refundable administration fee of £80 will be charged.

3.5 Requests submitted under the Data Protection Act 2018 Schedule 2 Part 1(2) (Crime and Taxation) will be free of charge and answered at the Council's discretion.

3.6 Requests for CCTV footage will be charged for as per the Council's CCTV Charging Policy.

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 £25.00 per hour.

7. Requests regarding the Deceased

7.1 Requests relating to deceased individuals will be charged at £25.00 per hour with a minimum payment of £75.00 payment for three hours' worth of work. This is a non-refundable administration fee. The Council is under no legal obligation to provide such records but will normally do so if the work is not too onerous and an administration fee is paid.