

Central Bedfordshire Council

Data Protection Policy

Issued by

Knowledge and Information Management

Version 1

February 2009

Not Protected

Policy Governance

Accountable Director	Director Of Business Transformation
Policy Author (Title)	Principle Information and Records Officer
Approved By (Title)	Shadow Executive Committee
Date Approved	17 February 2009
Issue Date	1 April 2009
Review Date	July 2009
Person Responsible for Review (Title)	Principle Information and records Officer
Include in Publication Scheme (Y/N)	Y
Publish to Web (Y/N)	Y
Circulation	<p>This policy is to be made available to all CBC staff and observed by all members of staff, both social care and otherwise.</p> <p>There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.</p>

Policy Approval

Central Bedfordshire Council (CBC) acknowledges that information is a valuable asset. It is therefore wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, in terms of protecting the interests of all of its stakeholders.

This policy and its supporting standards and work instructions are fully endorsed by the Council Executive through the production of these documents and their minuted approval.

I trust that all staff, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of the Council's objectives and the delivery of effective services to our community.

Chief Executive: _____

Date _____

The current version of the Central Bedfordshire Council's Data Protection Policy is available from the website at www.centralbedfordshire.gov.uk.

Alternatively, a copy can be obtained by writing to the Principle Information and Records Officer at:

Central Bedfordshire Council

Priory House

Chicksands

Shefford

SG17 5TQ

Revision history

Version Number	Revision Date	Summary of Changes	Author
0.1	6 September 2008	Draft	Rob Hutton
0.2	29 September 2008	Revision	Rob Hutton
0.3	2 October 2008	Revision	Rob Hutton
0.4	3 October 2008	Revision	Rob Hutton
0.5	28 November	Revision	Rob Hutton
0.6	8 December 2008	Revision	John Armstrong
0.7	13 January 2009	Revision	Rob Hutton
0.8	21 January 2009	Revision	Ken Thompson
0.9	28 January 2009	Issued for Approval	Rob Hutton
1.0	20 March 2009	Revisions required by Executive Committee	

Contents

- 1. Introduction**
- 2 Scope**
- 3 Rights and the Data Protection principles**
- 4 Roles and responsibilities**
- 5. Code of Conduct**
- 6. Identification and Reporting of Breaches**
- 7. Processing personal data**
- 8. Processing all personal data**
- 9. Processing sensitive personal data**
- 10. Notification**
- 11. Caldicott Principles**
- 12. Information sharing: general**
- 13. Information sharing across Bedfordshire and Luton**
- 14. Exceptional Disclosures**
- 15. Contracts with third parties**
- 16 Film and photographic images**
- 17. Closed Circuit Television (CCTV)**
- 18. Planning applications**
- 19. Subject access requests**
- 20. Valid Subject Access Requests**
- 21. Access to CCTV Footage**
- 22. Charges**
- 23. Appeals and role of the Information Commissioner**

- 24.1 Appendix A – Bedfordshire & Luton Information Sharing Protocol**
- 24.2 Appendix B – Data Protection Statement**
- 24.3 Appendix C – Data Protection Notification**
- 24.4 Appendix D - Related Council Policies**
- 24.5 Appendix E - Related Statutes, Legislation and Standards**
- 24.6 Appendix F – Document information**

Glossary

Advocate	A person who puts a case on someone else's behalf.
Caldicott Guardian	Senior role responsible for ensuring the Caldicott principles (see Information Governance Policy) are met.
Data Controller	A person or organisation who (either alone or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed: in this case Central Bedfordshire Council.
Data subject	A living individual to whom the personal data relates (e.g. service users, clients, employees). Generally anyone over the age of 12 is considered to be able to make a request on their own behalf.
Employee(s)	For the purposes of this policy employees of Central Bedfordshire will be referred to as Officers. see also Officers
Information Commissioner	Responsible for implementation and policing of the Data Protection Act and the Freedom of Information Act, with the authority to investigate and prosecute.
Non-sensitive Personal Data	Data about an individual that does not fall into the categories outlined in the definition of sensitive personal data.
Officer(s)	For the purposes of this policy, an Officer is defined as established members of staff, agency and temporary workers and consultants and contractors engaged for specific assignments and activities.
Personal Data	Any information, held manually or electronically, which relates directly to a Data Subject. This can include: Name and Address, Date of Birth, Qualifications, Income level, Employment history.
Processing	In relation to information or data, this means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: <ul style="list-style-type: none"> • organisation, adaptation or alteration of the information or data, • retrieval, consultation or use of the information or data, • disclosure of the information or data by

	<p>transmission, dissemination or otherwise making available</p> <ul style="list-style-type: none"> • alignment, combination, blocking, erasure or destruction of the information or data.
Sensitive Personal Data	<p>Personal data under the following headings:</p> <ul style="list-style-type: none"> a) race or ethnic origin b) political opinion c) religious or other beliefs d) trade union membership e) physical or mental health condition f) sexual orientation g) details of offences, court sentences or allegations under investigation
The Council	<p>For the purposes of this document this refers to Central Bedfordshire Council.</p>

1. Introduction

- 1.1 In collecting, processing, sharing and disposing of personal information relating to living individuals, the Council is bound by the Data Protection Act 1998 (the Act). This Act came into force on 1 March 2000. It repeals the Data Protection Act 1984, the Access to Personal Files Act 1987 and most of the Access to Health Records Act 1990. The Information Commissioner's Office enforces the Act, issues relevant guidance and registers personal data sets held by each organisation.
- 1.2 This document replaces any previous Data Protection policy documents created by this Council's predecessors.
- 1.3 Central Bedfordshire Council shall not be bound by previous decisions of Bedfordshire County Council, Mid Bedfordshire District Council or South Bedfordshire District Council.
- 1.4 Reference to any document, guidance note, act or regulation includes any amendment made from time to time.

2. Scope

This document sets out the Council's policy for compliance with the Act. Operational Procedures for responding to requests are outlined in the following guidelines:

- Officer Guidelines - Data Protection
- Elected Member Guidelines - Data Protection

3. Rights and the Data Protection principles

- 3.1 The Act creates a single framework for access to personal information about living persons held in both paper and electronic form. It enhances the rights of data subjects in that it confers a general right of access.
- 3.2 There are seven rights under the Act:
 - 1 The right to subject access:** This allows people to find out what information is held about them.
 - 2 The right to prevent processing:** Anyone can ask a Data Controller not to process information relating to them which causes substantial unwarranted damage or distress to them or to anyone else.
 - 3 The right to prevent processing for direct marketing:** Anyone can ask a Data Controller not to process information relating to him or her for direct marketing purposes.

- 4 Rights in relation to automated decision taking:** Individuals have a right to object to decisions made only by automatic means e.g. where there is no human involvement.
- 5 The right to compensation:** An individual can claim compensation from a Data Controller for damage and distress caused by any breach of the Act. Compensation for distress alone can only be claimed in limited circumstances.
- 6 The right to rectification, blocking, erasure and destruction:** Individuals can apply to a County Court (or the Information Commissioner) to order a Data Controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.
- 7 The right to ask the Commissioner to assess whether the Act has been contravened.**

Eight Data Protection Principles

- 3.3 From 1 April 2009 the Council is a registered Data Controller under the Act and will comply with the eight principles, which are defined as:
- 1** Personal data shall be processed fairly and lawfully.
 - 2** Personal data shall be obtained for one or more specified and lawful purpose and shall not be processed in any manner incompatible with that purpose or purposes.
 - 3** Personal data shall be adequate and relevant and not excessive.
 - 4** Personal data shall be accurate and up to date.
 - 5** Personal data shall only be kept as long as necessary.
 - 6** Personal data shall be processed in accordance with the rights of data subjects under the Act.
 - 7** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or destruction.
 - 8** Personal data should not be transferred to a country outside the European Union unless that country has an adequate level of protection for the rights and freedoms of the data subject.

4.Roles and responsibilities

Corporate Data Protection Officer

- 4.1 The employee designated as the Corporate Data Protection Officer has the corporate strategic responsibility for Data Protection in the Council, including:
- Undertaking the role of Corporate Data Protection Officer.
 - Maintaining notification of all the Council's datasets with the Information Commissioner's Office¹.

¹ Please note that Central Bedfordshire Council undertakes a separate notification for the handling and processing of electoral data

- Drafting guidance to process subject access requests made under the Act.
- Logging and monitoring the volume of Subject Access Requests and ensuring compliance.
- Ensuring appropriate and adequate training is delivered to Council officers/members.
- Providing technical support and guidance to Council officers as necessary.
- Escalating complaints relating to enquiries dealt with by Corporate Data Protection Officer to the Corporate Solicitor.

Caldicott Guardian

- 4.2 The role of the Caldicott Guardian is intrinsically linked with Data Protection as the information management requirements outlined in the Caldicott principles (see [Information Governance Policy](#)) deal with sensitive personal data.
- 4.3 The Caldicott Guardian should play a key role in ensuring that social care and partner organisations satisfy the highest practical standards for handling service user information. Acting as the “conscience” of an organisation, the Guardian should also actively support work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve.
- 4.4 The Caldicott Guardian also has a strategic role, that involves representing and championing confidentiality requirements and issues at Senior Management Team level and, where appropriate, at a range of levels within the organisations overall governance framework.
- 4.5 Note that the Caldicott Guardian’s role is specifically targeted towards Social Care/ Health information and records.

Key Responsibilities of the Caldicott Guardian

- agreeing and reviewing internal protocols governing the protection and use of service user-identifiable information by CBC staff.
- agreeing and reviewing protocols governing the disclosure of service user-identifiable information across organisational boundaries with partner organisations contributing to the local provision of social or healthcare services.
- a strategic role, developing security and confidentiality policy, representing confidentiality requirements at Board level.
- advising on annual improvement plans, and agreeing and presenting annual outcome reports.
- agreeing which staff should have access to what service user-identifiable information.

- to gatekeep and authorise levels of access to information systems storing or processing service user-identifiable information.
- to act as a resource for staff in matters of confidentiality and security of service user-identifiable information.

Service Managers

- 4.6 Service Managers or delegated officers are responsible for:
- Compliance with this policy and any associated procedures in handling Subject Access Requests.
 - Compliance with this policy and any associated procedures in the processing of personal information.
 - Providing access to case files following a request from a service user following appropriate verification.
 - Ensuring that any data transfer that takes place, whether hard copy or electronic, is necessary and is done so in the most secure and appropriate way.
 - Ensuring that when entering into any contracts with third parties that the contract includes a data protection clause specifying data controller and data processing roles and responsibilities.
 - Ensuring all officers under their direct supervision have undertaken mandatory Data Protection training and that this is refreshed in accordance with Council training schedules.

Head of Legal and Democratic Services

- 4.7 The Head of Legal and Democratic Services will:
- Be the ultimate legal responsibility for Data Protection compliance at the Council.
 - Deal with any issues that result in a conflict of interest involving the Corporate Data Protection Officer, for example, making a decision upon an appeal that relates to an action carried out by the Corporate Data Protection Officer.
- 4.8 The Head of Legal and Democratic Services will take reasonable steps to ensure that the Council's policies and procedures meet the requirement of the Data Protection Act.

Elected Members

- 4.9 Elected Members may process personal data in several capacities and their responsibility will reflect this:
- As elected members of the Council they may have access to and process personal data in the same way as employees. The data controller is the Council rather than the elected member.
 - When elected members act on their own behalf, the Information Commissioner's Office requires the elected member to notify in their own right as Data Controllers of this information. Examples include:

constituency casework, the processing of personal data in order to timetable surgery appointments or progress complaints made by local residents.

- When campaigning within their own political parties for adoption as a prospective candidate for a particular ward they act as individuals and can only rely upon the notification of their parties if as a matter of fact the parties control the manner and the purpose of the processing of personal data for the purpose of their individual campaigns.
- Ensuring any data transfer that takes place, whether hard copy or electronic, is necessary and is done so in the most secure and appropriate way.
- Ensuring that their knowledge of Data Protection is adequate to carry out their role as an elected member in accordance with the Act. If necessary, take advantage of existing Council training opportunities.

4.10 Further information can be found in the [Elected Member Guidelines - Data Protection](#).

Officers

- 4.11 Employees can be considered members of the public in terms of the right to make Subject Access Requests. However, as employees they have responsibility to:
- Process personal information in compliance with the Eight Data Protection Principles.
 - Make personal information available to Data Subjects following a valid Subject Access Request according to the Officer Guidelines - Data Protection
 - Ensure any data transfer that takes place, whether hard copy or electronic, is necessary and is done so in the most secure and appropriate way.
 - Ensure that they attend mandatory Data Protection training in accordance with Council training schedules.

5. Code of Conduct

- 5.1 All employees and members will receive copies of the Officer and Member Guidelines - Data Protection, the Working from home protocol and the ICT Acceptable Use Policy and guidelines.
- 5.2 Any employee who fails to comply with the above Policies and Guidelines may be subject to the Council's disciplinary procedure, dismissal where appropriate and possibly legal action.
- 5.3 Individuals whose information is held and processed by the Council can be assured that the authority will treat their personal data with due

care. It is possible that other legislation may (at times and under certain conditions) override Data Protection law – individuals should note that the Council will fulfil its legal responsibility.

6. Identification and Reporting of Breaches

6.1 Breaches in confidentiality must be reported to the Corporate Data Protection Officer as an incident so that they can be recorded and investigated. The Council's Caldicott Guardian must also be informed. Any training issues must be identified and addressed promptly.

6.2 Inadvertent breaches of confidentiality can occur. The following are examples:

- Discussion about a service user within or outside the organisation
- Reading confidential files when there is no requirement to do so
- Giving excessive information out when less would suffice
- Sending information in error e.g. to a wrong email address

6.3 If staff inadvertently breach confidentiality, they should inform their line manager, who will investigate the breach immediately and ensure it has been reported as a formal incident to the Corporate Data Protection Officer and to the Caldicott Guardian in writing. In case of a complaint by a service user or their representative, the Council's complaints procedure must be followed.

6.4 If undisclosed, a breach of confidentiality can result in disciplinary proceedings and, in serious cases, dismissal from employment. In addition, social care professionals may be subject to action by their regulatory bodies and possible legal action.

7. Processing Personal Data

- 7.1 The Council will process data in accordance with the [Eight Data Protection Principles](#). The Council shall:
- Only collect data necessary to carry out the defined function that the task relates to, and only hold and process personal data for the purposes of undertaking its statutory functions.
 - Only process data in accordance with the Council's Data Protection registration.
 - Respond to requests for access to personal data in 40 calendar days of receipt of appropriate verifiable identification (requests must be provided in writing).

- Only withhold information where exceptions under the Act permit.
- Treat all personal information with equal respect for confidentiality and security whether in written, spoken or electronic form.
- Seek consent to the sharing of personal or sensitive data, unless doing so would interfere with other statutory requirements, such as law enforcement.
- Only retain personal data for a specified time period defined by the Council's retention and disposal rules.
- Not delay data-sharing where it is necessary for the Council to protect the vital interests of a data subject, a minor or another person.
- Only use third parties to collect and process data where they can ensure confidentiality of data subjects' information and operate according the eight principles under the Act.
- Collect and process employee data in accordance with the Act and with [The Employment Practices Data Protection Code](#) issued by the Information Commissioner.

8. Processing all personal data

8.1 Schedule 2 of the Act describes a list of conditions, at least one of which must be met before personal data can be processed fairly and lawfully:

- The data subject has given his or her consent to the processing;
- The processing is necessary
 - for the performance of a contract to which the data subject is a party, or;
 - for the taking of steps at the request of the data subject with a view to entering into a contract;
- The processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract;
- The processing is necessary in order to protect the vital interests of the data subject;
- The processing is necessary;
 - for the administration of justice
 - for the exercise of any functions conferred on any person by or under any enactment
 - for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
 - for the exercise of any other functions of a public nature exercised in the public interest by any person.
- The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

9. Processing sensitive personal data

- 9.1 Schedule 3 of the Act provides an additional list of conditions, at least one of which must also be met before sensitive personal data can be processed fairly and lawfully.
- The data subject has given their explicit consent to the processing
 - The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment
 - The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent, or consent is being unreasonably withheld where it is necessary to protect the vital interests of another
 - The information contained in the personal information has been made public as a result of steps deliberately taken by the individual
 - The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice
 - The processing is necessary for the administration of justice or carrying out legal or public functions
 - The processing is necessary for medical purposes
- 9.2 Consent to collect sensitive personal data will be obtained by providing a comprehensive statement of the intended purpose(s) (see Appendix B) for which the sensitive personal data will be processed, together with an opt-in tick box or signature box by which the data subject can clearly indicate their consent for this data to be processed as described.

10. Notification

Council

- 10.1 In accordance with the Act the Council will undertake to notify the Information Commissioners Office of all the purposes that the Council will collect and process personal and sensitive personal data. This will be undertaken on an annual basis as required by the Act.

Electoral Registration Office

- 10.2 For the purposes of the Act, the Central Bedfordshire Electoral registration office is considered to be a separate legal entity. However, as the Electoral Registration Office acts as a part of the Council for day to day administrative purposes, the responsibility for renewing the

required notification and the management of the Act will be dealt with using the same channels as the Council.

Elected Members

- 10.3 For the purposes of the Act, elected members are considered separate legal entities and as such are responsible for ensuring that they have undertaken the notification process. Advice and assistance in achieving this is explained in the Elected Member Guidelines – Data Protection.

11. Caldicott principles

- 11.1 For all staff, but especially those handling confidential or sensitive service user information, the Caldicott Principles provide a framework for handling that information in a secure manner, which reduces the risk of compromise and harm.
- 11.2 The Principles are of particular importance if the information is being transmitted electronically from one point to another within the Council, or to another organisation. All staff should adhere to the following when making decisions about the handling or transfer of confidential information:
- 1 Justify the purpose for using confidential information
 - 2 Only use it when absolutely necessary
 - 3 Use the minimum that is required
 - 4 Access should be on a strict need to know basis
 - 5 Everyone must understand their responsibilities
 - 6 Understand and comply with the law

12. Information sharing general

- 12.1 Non-sensitive personal data provided to the Council may be shared across departments and services within the Council, and contractors employed by the Council, for legitimate Council activities such as:
- Recovering sums owed to the Council: rent and service charges, contractual payments, charges for the provision of any facility or service, application fees, fines, costs, or in respect of the recovery of any grant or overpayment made by the Council.
 - Updating Council records
 - Preventing and detecting fraud
- 12.2 In the case of sensitive personal information the Council will make every effort to obtain informed consent from the data subject. Consent assumes communication between the Council and the data subject and this may be through discussion; however, evidence of consent should then be obtained and held. Failure by the data subject to return a form requesting consent will not be assumed by the Council to imply consent.

12.3 In some cases, it may be necessary to disclose without consent in order to protect the vital interests of the data subject or other person, or where it has not been possible to obtain consent.

13. Information sharing across Bedfordshire and Luton

13.1 With effect from 1 April 2009 the Council will be a signatory to the Information Sharing Protocol for Bedfordshire and Luton (see appendix A).

13.2 If you need to establish an information sharing agreement with another organisation then you should consult with the Corporate Data Protection Officer and/or the Caldicott Guardian in the first instance.

14. Exceptional Disclosures

14.1 Exceptional Disclosure must be in compliance with statute. Circumstances in which disclosure may be required are:

- for the proper investigation of a complaint, staff disciplinary matter, untoward incident or claim.
- for the prevention, detection or prosecution of a serious crime or in line with the Crime & Disorder Act 1998 protocol.
- to safeguard national security.
- for the protection of public health - e.g. in the prevention and control of communicable diseases NOT covered by public health legislation.

14.2 The following Acts provide for circumstances where disclosure without consent is required:

- Births and Deaths – National Health Service Act 1977
- Notifiable Communicable diseases – Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place – Health and Safety Act
- Offenders thought to be mentally disordered – Mental Health Act
- Child Abuse
- Drug Addicts – Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents – Road Traffic Act
- The Crime and Disorder Act 1998

14.3 Disclosure can be required by order of a Court including a Coroner's Court.

- 14.4 Should there be a doubt as to the procedure or the basis for the request, the responsible social care professional is encouraged to discuss the matter with the Caldicott Guardian or their line manager in the first instance.

15. Contracts with third parties

- 15.1 In the event that the Council enters into a contract with a third party which involves collecting, processing, handling, securing or disposing of information at any level there should be a data protection clause inserted into said contract.
- 15.2 This clause will identify the roles and responsibilities of the data controller and data processor in relation to activities carried out during the life, and after termination of, the contract.

16. Film and photographic images

- 16.1 The Council undertakes filming and photography in various capacities (with the exception of CCTV see section 3.6). In most cases any officer should seek to have the written permission of any individual involved prior to taking any images.
- 16.2 In the case of events that take place on Council premises the invitation should include a statement that filming or photography will take place and by attending the event the individual is giving consent to appear in images that could be used as publicity. It is the responsibility of the individual to avoid a clearly designated photographer or cameraperson should they not wish to be the subject of any individual focus.
- 16.3 The majority of these images will be acquired for the purpose of publicity and will be made public in newsletters, or the Council website. If consent has not been given then the image should not be taken.

17. Closed Circuit Television (CCTV)

- 17.1 The Council uses CCTV in and around Council owned buildings, and in public access areas. The use of these cameras is for the following reasons:
- to help reduce the fear of crime
 - to help deter crime
 - to help detect crime and provide evidential material for court proceedings
 - to assist in the overall management of the district
 - to enhance community safety, assist in developing the economic well being of the district and encourage greater use of the Town centres, Theatre, leisure Facilities, Car Parks and Open Park Area

- to assist with traffic management
- to assist in supporting civil proceedings which will help detect crime
- to assist in the training of CCTV operator, the police and others involved in the use of the CCTV system.

17.2 The majority of CCTV cameras will only be used for the purposes of preventing and detecting crime or of preventing disorder. CCTV may on occasion be used to target individuals in conjunction with the aforementioned purposes. For this purpose, however, the Regulation of Investigatory Powers Act 2000 must be adhered to.

18. Planning applications

18.1 The planning application process requires that non-sensitive personal data is placed in the public domain as part of the process of ensuring that the application meets the requirements of the Town and Country Planning Act 1990. In all cases the applicant is made aware that this data is to be placed in the public domain as part of the process and agrees to it being thus made public.

18.2 Where planning applications are submitted with supporting sensitive personal data, such as medical information, the following criteria must be satisfied in the case where the information supports the application:

- a. The application is accompanied by a depersonalised synopsis of the medical data.
- b. A written and signed agreement of the data subject has been received that states that this synopsis can be placed into the public domain as part of the application.

Or

- a. Original documentation has been received and redacted by the applicant to remove any non-relevant information such as NHS Numbers.
- b. A written and signed agreement of the data subject has been received that states that this data can be placed into the public domain as part of the application.

18.3 Under no other circumstances will the Council place any sensitive personal data obtained through the planning application process in the public domain.

19. Subject access requests

19.1 Data subjects have a right of access to information about themselves that includes factual information, expressions of opinion, and the intentions of the Council in relation to them, irrespective of when the information was recorded. The Council will disclose any information

they hold on a data subject (applying any necessary exemptions) within 40 calendar days of receiving a valid Subject Access Request.

Proof of identity

- 19.2 To protect the data subject and avoid disclosing data to unauthorised persons the Council will require proof of identification and address from the requester prior to releasing the data. Such proof must be hand-delivered; however, in circumstances where this is not practicable, alternative arrangements will be determined on a case-by-case basis. For more information see the Officer Guidelines - Data Protection.

Requests from advocates

- 19.3 Data subjects can also make a request for information through a representative or agent such as a solicitor; such representatives must have the written consent of the data subject. The Council will ask for proof that consent from the data subject has been received, and for proof of identification of the Data Subject and Advocate. A record of this consent must be held on file. For more information see the Officer and Elected Member Guidelines - Data Protection.
- 19.4 If a person does not have the capacity to manage their own affairs, a person acting under an order of the Court of Protection or who has Enduring Power of Attorney/ Lasting Power of Attorney can request access on her or his behalf. People with learning disabilities or mental health problems do not necessarily lack the mental capacity to make a subject access request on their own behalf. Such requests require a judgement to be made on a case-by-case basis.

Requests relating to employees

- 19.5 The Council, in accordance with the Information Commissioner's guidance (published from time to time) will disclose information identifying Council employees and ex-employees acting in their official capacity of Council officer, such as name, job title and work phone number. If a third party organisation or individual, such as a contractor, therefore, has provided information to the Council in carrying out its business function for and on behalf on the Council, this information is eligible for disclosure.

Disclosure without consent

- 19.6 The Council will make reasonable endeavours to obtain consent prior to disclosure unless this would interfere with a statutory obligation. If consent is not given because the person is either unable or unwilling to give that consent, then the information will only be released where the Council considers it is legally or statutorily obliged to do so.

20. Valid Subject Access Requests

20.1 Subject Access Requests should be submitted to the Customer Relations and Access to Information Team for logging and processing. Enquiries can be made via the following channels:

- **In person:** At Council offices or Points of Presence
- **By post:** addressed to the Principle Information and Records Manager
- **By fax:** <INSERT FAX NUMBER>
- **By email:** accesstoinfo@centralbedfordshire.gov.uk

20.2 Data subjects should describe as precisely as possible the information they wish to access, including where relevant:

- Date of birth
- Any previous addresses within the district they have lived in, and
- List of service areas they think may hold information about them

20.3 Requests for personal information will be processed in line with the requirements of the Act and Council procedures.

21. Access to CCTV footage

21.1 The Council remains the Data Controller of any CCTV footage created by any equipment owned by the Council. It will provide access to this footage in accordance with the principles of the Act in cases where the individual can clearly be identified.

21.2 The Council will endeavour to assist any investigation by the police, under Section 29 of the Act. However it will reserve the right to refuse access as Data Controllers if it is considered that providing access to the footage will contravene the Act.

21.3 Access to CCTV footage will be via a set procedure following a written request. This procedure complies with the 'Code of Practice for the Operation of Closed Circuit Television' as amended from time to time.

21.4 See paragraph 22.3 below regarding charges for releasing CCTV footage.

22. Charges

General Charges

22.1 The Council reserves the right to apply fees as specified by other relevant legislation.

Council officers

- 22.2 The Council will not apply the fee to Council Officers wishing to access their employment information whilst they are still employed by the Council.

Subject access requests

- 22.3 In most cases, the Council will not apply a fee. However, the exception to this is a request for CCTV footage where there is a direct cost in physically providing the information, and a £10 fee will be applied.
- 22.4 The Council also retains the right to apply a fee (currently set at £10) at its discretion where it is permitted to do so.

23. Appeals and role of the Information Commissioner

- 23.1 In the event of a complaint or challenge regarding the application of an exemption, the initial request, decision audit trail, correspondence and information released will be reviewed independently by the Head of Service for Legal and Democratic Services.
- 23.2 If the requester is dissatisfied with the appeal outcome they may seek an independent review by the Information Commissioner. The Information Commissioner has the authority to demand disclosure from the Council.
- 23.3 The [Information Commissioner](#) is an independent official appointed by the Crown to oversee the Act. Any person may apply to the Information Commissioner for an assessment of whether data collection and processing is being carried out in compliance with the Act. In the first instance however the Information Commissioner will usually expect that Data Subjects will have taken the matter up with the Council first.
- 23.4 The Council will take into account all notices and guidance issued by the Information Commissioner.

24.1 Appendix A – Information Sharing Protocol for Bedfordshire and Luton

<INSERT LINK TO INFORMATION SHARING PROTOCOL ON CBC WEBSITE>

24.2 Appendix B – Data Protection Statement

The following statement must be printed on any Council documents that are intended for the purpose of collecting personal data.

“The information submitted in this document was collected for the following purposes:

<INSERT REASON/S FOR COLLECTING DATA>

Central Bedfordshire Council ensures any personal data collected will be retained securely for as long as necessary, and only used for legitimate Council activities to facilitate the delivery of Council services, or for the purpose of preventing and/or detecting fraud and/or crime, in accordance with the Data Protection Act 1998.

Central Bedfordshire Council's Data Protection policy is available from the website at www.centralbedfordshire.gov.uk or by writing to the Corporate Data Protection Officer at **<INSERT CONTACT DETAILS>**“

24.3 Appendix C – Data Protection Notification

Central Bedfordshire Council annually renews its registration of notification of purpose under the Data Protection Act. The current details of the notification can be viewed on the Register of Data Controllers via the Information Commissioners Website at the following address:

www.ico.gov.uk/Home/tools_and_resources/register_of_datacontrollers.aspx

The Central Bedfordshire Council Registration Number is as follows:

<INSERT NOTIFICATION NUMBER>

24.4 Appendix D - Related Council Policies

1. Information Governance
2. Freedom of Information
3. Environmental Information Regulations
4. Re-use of Public Sector Information
5. Information & Records Management
6. Information Security
7. ICT Acceptable Use Policy

24.5 Appendix E - Related Statutes, Legislation and Standards

Legislation	Notes	Area of impact
The Data Protection Act 1998	The Data Protection Act requires that all personal information be handled in an appropriate way.	Access to Information Data Management Records Management Information
Freedom of Information Act 2000	Provides the legal framework around which the public are able to access information held by the Council. Section 46 – of the Freedom of information act makes it clear that in order to comply with the Fol a public body must maintain its records in a way that makes the accessible.	Access to Information/Records Management
The Environmental Information Regulations 1992	Provides the framework for public access to Environmental information of an organisation Pt2 Section 5 (4) – requires that information is accurate and up-to-date and comparable	Access to information/ Management of environmental information
Human Rights Act 1998	Article 8.1 of the European Convention on Human Rights (given effect via the Human Rights Act 2000) provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. However there are exemptions that override those rights, such as national security, public safety, prevention of disorder or crime, and protection of the rights and freedom of others.	The Council has a duty to abide by the human rights act and ensure that all correspondence with the Council is treated appropriately, which includes managing it in a way that will not invade the privacy of the individual.
Crime and Disorder Act 1998	Section 115 of this Act provides that any person has the power to disclose information necessary for the provisions of the Act to the police, local authorities, probation service or health authorities.	To be able to provide appropriate information the Council must not only ensure access to the information, but that the context is not lost through poor management.
Children Act 2004	Background Every Child Matters: Change for Children	Information retained in all service areas could

	(Dec 2004), and the draft statutory guidance on the Children Act 2004 S10 Duty to Cooperate (Dec 2004), set out clear expectations for local action to improve information sharing. It seeks to provide clarity on the legal framework for practitioners sharing information about children, young people and families; and give practitioners confidence in making decisions.	potentially be valuable in ensuring the well being of children in the area. Therefore being able to access information from a wide range of sources across the Council is essential.
Limitation Act 1980	This act places a limit on the validity of information, therefore provides the legal framework for retention and disposal of certain documents	Retention and disposal of records, although not all records or information has a legal limitation attached.
Public Records Acts 1958 & 1967	These two acts provide the framework for the appropriate management of Public Records, these were heavily amended in with the introduction of the Freedom of Information Act	Management of Public Records
Local Government (Records) Act 1962	(10 A local Authority may do all such things as appear to Power to it necessary or expedient for enabling adequate use to be made of records under its control, and in relation to such records may particular – a) Make provision for enabling persons, with or without charge and subject to such conditions as the authority may determine, to inspect the records and to make or obtain copies thereof	Records Management
Taxes Management Act 1970	Details the requirements for managing tax records	Records retention
Local Government Act 1972	Section 224 – without prejudice to the powers of the <i>custos rotulerum</i> to give directions as to the document of any county, a principle Council shall make proper arrangements with respect to any documents, which belong to or are in the custody of the Council or any of their officers	Records Management

Codes of Practice	Notes	Area of impact
<i>FOI Code of Practice for Local Government</i>	<p>“1. To set out practices which public authorities, and bodies subject to the Public Records Act 1958 and the Public Records Act (NI) 1923, should follow in relation to the creation, keeping, management and destruction of their records (Part I of the Code); and</p> <p>2. To describe the arrangements which public record bodies should follow in reviewing public records and transferring them to the Public Record Office...”</p>	Access to Information

Standards

ISO 15489-1 and ISO 15489-2, 2001 ‘best practice’ for managing records in an organisation.

PD 0008:1999 a code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically

PD 0010:1997 Principles for Good Practice for Information Management

BS 5454:2000 Recommendations for the Storage and Exhibition of Archival Documents,

ISO 18925:2002 Imaging materials – optical disk media – storage practices

PD 0016:2001 Guide to scanning business documents

MoReq 2001 Model requirements for the management of electronic records.

BS 7799:2002 Specification for information security management

24.6 APPENDIX F - Document Classification

All corporate documents are classified using the two following classification methods. For more detailed information see [Corporate Information Records Management Policy](#).

24.6.1 Security Classification

The purpose of security classification is to ensure that all information is secured and only accessible to the appropriate persons. All documents (including emails) will have the security classification clearly identified.

The security classification is divided into the following three categories:

- Not Protected
- Protected
- Restricted

Refer to [Information and Record Management Policy](#) for a detailed explanation of the security classifications.

The security classification of this document is as follows:

- Not Protected

24.6.2 Functional Classification

The purpose of Functional Classification is to ensure that all significant documents are placed in their correct position within the corporate information architecture. This is to facilitate effective management, access and disposal of information across the organisation. Each document will be marked using the corporate function (highest element of classification which describes the general area in which the document resides) under which it falls.

The functional classification of this document is as follows:

- Information Management