Data Protection Policy

Document Control

Organisation	Rutland County Council
Title	Data Protection Policy
Author	Lisa Wakeford
Owner	Head of Business Support Places
Protective Marking	Unclassified
Approval Date	7/2/11

Revision History

Revision	Reviser	Previous	Description of Revision
0.1	Phil Naylor	N/A	Initial Draft
0.2	Lisa Wakeford	0.1	Final Draft

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
SMT	Debbie Muddimer	7/2/11

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
ALL STAFF	N/A	N/A

Contributors

- None

Data Protection Policy

Rutland County Council

Contents

1.0 Introduction

This document is designed to help RCC employees gain an awareness of what is required of them to comply with the Data Protection Act 1998. It is the intention of SMT that data protection is a high priority and that good practice within data protection is a vital part of the service that RCC provides. The Data Protection Act is not a barrier to sharing information, but a framework to ensure that personal information is managed appropriately.

Rutland County Council needs to collect, hold, process, retain and share personal information about people with whom it deals in order to carry out its business and provide its services. Such people include service users, council tax and business rate payers, employees (present, past and prospective), suppliers and other business contacts. The information could include such details, as name, address, date of birth, e-mail address etc.

Although this policy provides guidance on good practice for all members of staff in the protection and use of personally identifiable information, to ensure that RCC meets its obligations under the Data Protection Act 1998 legislation, it cannot provide definitive answers for every situation. Much depends on the context of the individual case.

2.0 Scope

This policy applies to all personal identifiable information, whether written, computerised, visually or audio recorded. All personal identifiable data is included, this covers data such as personnel, finance, contractors, suppliers, volunteers and any other recognised data systems are also covered.

This policy applies to elected members and all employees of the Council, and to partner agency employees (including consultants, volunteers and contractors) handling data on behalf of the Council. Every person handling personal data must understand and comply with the principles of the Data Protection Act 1998. Individuals are personally liable for breaches of the Act.

RCC will, through appropriate management, ensure compliance with the Data Protection Act. This means that RCC will:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of people about whom information is held, are able to be fully exercised under the Act.
- Take appropriate technical and organisation security measures to safeguard personal information;

- Ensure that personal information is not transferred outside the EEA without suitable safeguards

In addition RCC will ensure:

- There is a designated person with specific responsibility for data protection within the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information has appropriate managerial support;
- Anybody wanting to make enquires about handling personal information knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are clearly described;
- A regular review and audit is made of the way personal information is managed;

3.0 Policy Statement

RCC is committed to complying with the Data Protection Act (1998) to preserve:

- Confidentiality: Protecting sensitive information from unauthorised disclosure;
- Integrity: Safeguarding the accuracy and completeness of information;
- Availability: Ensuring that information and vital services are available to authorised users

and to ensure that any person identifiable information received, stored, processed and transmitted is done so in a secure environment.

This policy will support and link appropriately with the IT Security Policy.

4.0 Management Responsibility

The Chief Executive has overall responsibility for the Data Protection Policy within RCC. The implementation of, and compliance with, this Policy is delegated to the Strategic Director for Resources.

The Policy will be reviewed bi-annually or more frequently if appropriate to take into account changes to legislation which may occur, and/or guidance from the Office of the Information Commissioner (OIC).

The day to day responsibilities for enforcing the Policy will be devolved to the Head of Business Support Places.

All new starters will be given Data Protection and confidentiality training as part of the induction process. Extra training in these areas will be given to those who require it. A register will be maintained of all staff attendance at training sessions.

Temporary employees and contractors will be issued with a Contract which will bind them to the RCC terms and conditions concerning Data Protection a copy of which is available from the Human Resources Department and on the IT Service Desk Customer Portal.

Responsibility for the Data Protection Act cannot be sub-contracted, therefore it is the Council's responsibility to ensure the security of personal data. Contracts must include measures to ensure data is handled appropriately and used for agreed purposes. Contractors are required to follow Council policy and should be provided with the minimum information needed to carry out work on its behalf.

5.0 Definitions

Personal data is information which relates to a living individual who can be identified.

A **data subject** is an identifiable living individual.

A **data controller** is a person or organisation who determines the purposes for which data are to be processed and the manner in which that data are processed. A data controller may also process data on behalf of another (e.g. Police, Health Service and suppliers). Rutland County Council is a data controller.

6.0 Notification

The Information Commissioner's Office maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the types of personal information they process. Individuals can check the register to find out what processing of personal information is being done by a particular data controller. Notification is the process by which a data controller's details are added to the register.

RCC will maintain and keep their registration accurate and up to date, conducting annual reviews.

7.0 Legal Context and disclosure

Reference to the following legislation and guidance may be required when reading or applying this policy:

- The Human Rights Act 1998 and the European Convention of Human Rights (see Appendix 1)
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Mental Capacity Act 2005
- The Education (Pupil Information)(England) Regulations 2000
- The Caldicott Principles (Social Care only)

In addition, reference must be made to Common Law Duty of Confidentiality (see Appendix 3).

7.1 Disclosures under the Crime and Disorder Act

In situations where disclosures to the police may become routine, a formal protocol should be developed and agreed between the organisation and the police, so that all staff involved know what to do.

Note that the Crime and Disorder Act 1998 does not in itself constitute a statutory requirement for RCC to disclose information to other agencies.

7.2. Enquiries from relatives and friends

Information should only be disclosed to relatives, friends or carers if the data subject has given consent. Wherever possible, the express consent of the data subject (which may be oral or written) should be obtained and documented. If consent is not possible, then the Officer who is currently or was most recently responsible for the data subject, or the departmental manager, can make the decision on whether to disclose information.

No one with access to confidential information should pass on any information to their own relatives or friends, or seek to find out details about themselves. No information should be passed on for personal or commercial gain.

7.3. Anonymised information

The removal of personal details alone may be sufficient to protect a data subject's identity. If anonymisation is to be relied upon as the condition for disclosure without consent, it requires the removal of any information that could allow identification of the data subject by any means. For some uses of data, the retention of service number or system code, may be acceptable if recipients of the data do not have access to the 'key' to trace the identity of the data subject. Such pseudonymisation may, with appropriate safeguards, may be sufficient to allow use without express consent. It is good practice to inform people that their information may be used anonymously.

7.4. Research

The use of RCC's information for research is subject to the usual principles of data protection. Wherever possible, anonymous data or data with coded identifiers should be used. In addition to this SMT should approve all releases of personal data for research project. Prior to seeking approval the Data Protection Officer should provide written support.

Any party wishing to use RCC data for research purposes should sign a confidentiality agreement. A statement relating to Data Protection and Confidentiality should appear in all contracts e.g. honorary contracts.

7.5 Information Sharing with other organisations

When data is collected a Privacy Notice must clearly explain what data we expect to share, who it is likely to be shared with and in what circumstances.

- Non-sensitive personal data may be shared across Council departments and with partners and contractors working on the Council's behalf for legitimate purposes.
- Sensitive personal data will only be disclosed with the informed explicit consent of the data subject, and the signed consent form must be retained on the relevant case file. In some cases verbal consent may be given and this must be recorded accurately within the relevant case file. Consent cannot be assumed by a non-response to a request for consent.
- There are circumstances in which personal data may be disclosed without obtaining the data subject's consent such as safeguarding the data subject or others, and to assist with the prevention and detection of crime. Wherever possible, express informed consent for sharing sensitive personal data will be sought from the data subject. Where this is not possible or contrary to the public interest, the Council will ensure that the sharing of data meets the relevant condition or exemptions from the non-disclosure provision contained within the Act.
- Information Sharing protocols exist between the Council and partnership agencies such as the Police, the NHS and voluntary organisations. Employees must refer to these protocols when considering whether to disclose personal data in order that standard procedures are followed. Please refer to The Leicestershire wide Information Sharing Policy. Available on the IT Service Desk Customer Portal. This policy covers information sharing between public sector organisations.

7.6 Disclosure in the public interest

When considering disclosing information to protect the public interest, officers must:

- Consider how the benefits of making the disclosure balance against the harms associated with breaching a data subject's confidentiality
- Assess the urgency of the need for disclosure
- Consider whether the subject might be persuaded to disclose voluntarily
- Inform the subject before making the disclosure and seek his or her consent, unless to do so would enhance the risk of harm or inhibit its effective investigation
- Reveal only the minimum information necessary to achieve the objective
- Seek assurances that the information will be used only for the purpose for which it was disclosed
- Be able to justify the decision – this should be clearly documented.

It is advisable to discuss situations on an anonymous basis with colleagues, the Caldicott Guardian and the manager/Head of Service, and/or to seek advice from professional and indemnifying bodies. It is important not to equate "the public interest" with what may be "of interest" to the public.

8.0 Subject Access Procedure

All requests from individuals to have access to information must be sent to the Data Protection Officer who will ensure that RCC complies with the requirements of the Act regarding subject access rights.

All requests for formal access should be made in writing, enclosing relevant identification. If a telephone request for data is received, the subject access procedure will be explained and the relevant application form sent to the data subject. Having received a request, the data controller must not make any special amendment or deletion that would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the data subject.

The individuals will be provided with information about the processing of their data as well as a copy of their data. Information should be provided in a permanent format unless this is not possible, would involve disproportionate effort or the data subject agrees otherwise. The information should be intelligible and any codes, abbreviations and acronyms should be explained.

Data subjects have a right to receive information held about them within 40 days. RCC will charges the Statutory fee of £10 per request.

9.0 Freedom Of Information Act 2000

The Freedom of Information Act 2000 ('the Act') was passed on 30 November 2000. The Act will be enforced by the Information Commissioner, this role now combines Freedom of Information and Data Protection. Both the Freedom of Information Act and the Data Protection Act relate to

information handling and the dual role will allow the Commissioner to provide an integrated and coherent approach.

The Act gives a general right of access to all types of 'recorded' information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Anyone will be able make a request for information, although the request must be made in writing, which includes emails. The request must contain details of the applicant and the information sought. The Act gives applicants two related rights:

- To be told whether the information is held by the public authority
- To receive the information (and where possible, in the manner requested, i.e. as a copy or summary, or the applicant may ask to inspect a record).

Public authorities will be obliged to provide information recorded both before and after the Act was passed.

Personal identifiable information is still governed by the Data Protection Act.

10.0. Overseas Transfers

Overseas transfers of data will also be kept to the absolute minimum necessary to perform their function. Data will not be transferred outside of the European Economic Area without such written authorisation.

RCC will ensure that robust written contracts are in place with any party that processes RCC's data outside of the EEA.

11.0. Security

Data controllers must take appropriate security measures to safeguard personal data. The 1998 Act requires that data controllers must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data. Where a controller uses the services of a data processor the security arrangements must be part of a written agreement between the two.

RCC will strive to ensure that adequate security measures are in place to guarantee that all personal data is stored, processed, disposed of or disclosed in a manner which prevents access by any unauthorised persons.

RCC is committed to working towards the ISO17799 information security standard. ISO17799 was developed as a result of industry, government and commerce demand for a common framework to enable companies to develop, implement and measure effective security management practice and to provide confidence in inter-company trading. It is based on the best current information security practices of leading British and international businesses and has met with international acclaim.

RCC has a separate Information Security Policy, which details RCC's security arrangements in further detail.

12.0. Records Management

Each service area must manage its records in accordance with the Council's policies and procedures. It is essential that records are stored securely and the location of files is up to date at all times. Effective methods of security must be in place to help prevent the inappropriate disclosure or loss of personal data. Staff or other representatives working off-site from Council offices must ensure records are adequately protected at all times, preventing damage, theft/loss and unauthorised access to personal data.

All records must be accurate, up to date and not excessive, and any corrections or amendments to a record are to be made in accordance with departmental procedures, providing a clear audit trail. The disposal of data is to be completed using the document retention and disposal schedules.

Electronic data is managed within the procedures described in the Council's IT Security policy.

13.0. Elected Members

Elected members may have access to and process personal data in the same way as employees, and must comply with the Act and the eight Data Protection principles. Since data held on Council systems may be used by Elected Members in their other roles the data controller may be the Elected Member or the Council individually, jointly or on behalf of the other.

Notification of data controller responsibility must be arranged as follows:

- When acting on behalf of the Council, Members can rely on the Council's notification
- When acting on their own behalf (e.g. when dealing with complaints made by local residents) Members must notify the Information Commissioner's Office in their own right
- When campaigning within their own political party, Members may rely on the notification made by their party

14.0 Local Authority Maintained Schools

Schools are individually responsible for their own compliance with all aspects of the Data Protection Act 1998, including management of policies and practices.

15.0 Breaches Of The Act

A breach of the Act may arise from a theft, accidental loss by an employee, a deliberate attack on the Council's systems, unauthorised use of personal data by an employee or equipment failure.

In the event of a breach it is essential that the Council's Data Protection Officer or in their absence, another senior manager is informed immediately. Resulting actions will require that all risks are identified, the appropriate people and organisations are informed of the breach, and communication is prepared to help prevent damage to the Council's reputation.

16.0 Dissemination/circulation of the policy

The policy will be disseminated via E-mail to all employees and Councillors.

Appendix 1

THE DATA PROTECTION ACT (1998) PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

   - At least one of the conditions in Schedule 2 is met and
   - In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Conditions for Processing - Schedule Two of the Act

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject
- To comply with any legal obligation to which the data controller is subject
- To protect vital interests of the data subject
- To perform public functions
- To pursue legitimate interests of the data controller unless prejudicial to the interests of the data subject

Conditions for Processing Sensitive Data - Schedule Three of the Act

At least one of the Schedule Three Conditions must be satisfied, in addition to at least one of the Schedule 2 conditions before processing of sensitive personal data can claim to have been lawful in accordance with the First Principle of the Act.

- Explicit consent of the data subject
- To comply with employers legal duty
- To protect the vital interests of the data subject or another person
- Performed by certain non-profit bodies
- The information has been made public deliberately by the data subject
- In legal proceedings and in the exercise of legal rights
- To carry out public functions
- For medical purposes
- For equal opportunities monitoring
- As specified by order

Sensitive Personal Data

The Act introduces categories of sensitive personal data, namely personal data consisting of information as to:

- racial or ethnic origin of the data subject
- political opinions
- religious beliefs or other beliefs of similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- the commission or alleged commission by them or any offence or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

Appendix 2

The Human Rights Act 1998 and the European Convention of Human Rights

The European Convention on Human Rights has been interpreted to confer positive obligations on public authorities to take reasonable action within their powers (which would include information sharing) to safeguard the Convention rights of people. These rights include the right to life (Article 2), the right not to be subjected to torture or inhuman or degrading treatment (Article 3) and the right to liberty and security (Article 5).

Article 8 of the European Convention on Human Rights was incorporated into UK law by the Human Rights Act 1998 and recognises a right to respect for private and family life:

- Article 8.1: Everyone has the right to respect for his private and family life, his home and his correspondence.
- Article 8.2: There shall be no interference by a public authority with exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, protection of health and morals or for the protection of rights and freedoms of others.

Sharing confidential information may be a breach of an individual's Article 8 right: the question is whether sharing information would be justified under Article 8.2 and proportionate.

The right to a private life can be legitimately interfered with where it is in accordance with the law and, for example, is necessary for the prevention of crime or disorder, for public safety or for the protection of health or morals, or for the protection of the rights and freedoms of others. Consideration is required for the pressing social need and whether sharing the information is a proportionate response to this need and whether these considerations can override the individual's right to privacy. If a person is at risk of significant harm, or sharing is necessary to prevent crime or disorder, breach of the person's right would probably be justified under Article 8.

Appendix 3

Common law duty of confidentiality

The common law duty of confidentiality is explained in sections 3.6 to 3.12 of the central government guidance *Sharing information: practitioners' guide*. The common law provides that where there is a confidential relationship, the person receiving the confidential information is under a duty not to pass on the information to a third party. The duty is not absolute and information can be shared without breaching the common law duty if:

- the information is not confidential in nature; or
- the person to whom the duty is owed has given explicit consent; or
- there is an overriding public interest in disclosure; or
- sharing is required by a court order or other legal obligation.