SOUTH KESTEVEN DISTRICT COUNCIL
DATA PROTECTION POLICY

Document Location

This document will be held on the internal ICT server.

Revision History

Date of this revision: 24th March 2015
Date of Next revision: October 2017

Revision date	Previous revision date	Summary of Changes	Changes marked
2.11.11	10.10.08	First draft	
15.09.14	02.11.11	Second draft	
24.03.15	15.09.14	Third draft	Section 11 home - working and introduction of protocol at Annex 2

Approvals

This document requires the following approvals.

Name	Title	Date of Issue	Version

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version
	Business Managers		
	Executive Managers		
	Strategic Directors		
	Chief Executive		
	Cabinet		
	Engagement PDG		

	All staff		

CONTENTS

Appendix 1 – Non- Disclosure Agreement

Appendix 2 -

1. Introduction

1.1 This is a statement of the Data Protection Policy adopted by **South Kesteven District Council**.

1.2 **The Council** needs to collect and use certain types of information about the people with whom it deals, as part of its day-to-day business activities. These people typically include current, past and prospective employees, suppliers, consultants and contractors, tenants, residents, customers, applicants for services and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of Government Departments, for example, to prevent fraud or other types of crime. Such personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in accordance with the Data Protection Act 1998. ("The Act"). We regard the lawful and correct treatment of personal information as very important both to the successful management of our operations, delivery of services and to maintaining the confidence in us of those with whom we deal. We will ensure that our organisation treats personal information lawfully and correctly.

1.3 To this end, we fully endorse and adhere to the principles of Data Protection, as described in the Data Protection Act 1998 ("the Act").

1.4 In order to ensure that there is someone with specific responsibility for Data Protection Andy Nix/Lucy Youles have been appointed as Data Protection Officers and each department of the Council has nominated a Data Protection representative (**see Section 7 below).**

1.5 If anyone would like more information about the Act or its Policies please contact Legal Services or any of the Data Protection representatives.

2. Terms Used

2.1 Within this policy and the Act itself, a number of terms are used and these are described below. It is recommended that you look at the terms used to fully understand the guidelines that follow.

2.2 **Personal data** – any personal information - held either electronically or manually - which relates directly to a Data Subject and includes:

- name and address
- date of birth
- qualifications
- income level
- employment history
- an opinion about an individual

2.3 **Sensitive personal data –** this is information held ether electronically or manually relating to a living person and that information relates to:

- racial or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- health
- sexual life
- criminal allegations, proceedings or convictions

2.4 **Data Controller –** describes those who collect and use personal data – namely South Kesteven District Council or the Electoral Registration officer and those who have a Notification registered with the Information Commissioner

2.5 **Data Subject –** a living individual about who personal data is held.

2.6 **Notification –** The Information Commissioner maintains a public register of data controllers. Each record on the register includes the name and address of the data controller and a general description of the information they process. Each department within this Council must give notification – the process by which the data controller's details are added to the register - to the Information Commissioner, setting out the information they hold.

2.7 **Information Commissioner –** The government body responsible with the implementation and the policing of the Data Protection Act 1998. They have authority to both investigate and prosecute on behalf of any individual who believes that their personal data is not being handled in accordance with the Act.

2.8 **Processing data –** can mean anything from simply holding data to passing it on in any form to other people

3. The Purpose of the Policy

3.1.1 The Council's Data Protection Policy ("The Policy") sets out the rules and procedures to be followed when processing personal data.

3.1.1 All the Council's Departments, Offices and Employees must observe the following provisions of this Policy.

3.1.2 The purpose of the Policy is:

- to ensure the Council's services follow the provisions of the Data Protection Act 1998 and all the relevant subordinate Data Protection Legislation

- to ensure that personal data is effectively managed and processed in a fair, lawful and consistent manner within the Council's services

- to ensure that all members of staff and Councillors within the Council's services are aware of their duties and obligations under The Act and the possible consequences of breaches of The Act

- to ensure that the names and contact details of the members of staff who have responsibility for advising and assisting departments with compliance of The Act are published and accessible

4. The Data Protection Principles

4.1 The Act sets out the following eight Data Protection principles that represent the core duties imposed on the Data Controller (i.e. SKDC), which have to be complied with when processing personal data:

- obtain and process personal data fairly and lawfully
- use it only for defined purpose(s)
- make sure it is adequate, relevant and not excessive
- keep it accurate and up to date
- delete it when no longer required
- process in accordance with the data subject's rights
- keep it secure
- do not transfer it to other countries without adequate protection

4.2 **The First Principle - Personal Data has to be processed fairly and lawfully**

4.2.1.1 In order to comply with the first Data Protection principle, the Council's services must ensure that:

- Personal Data are processed on the basis of one or more of the limited number of conditions for processing set out in The Act (see paragraphs 4.2.3 to 4.2.7)
- Processing, and in particular obtaining of personal data is fair to the data subject concerned

4.2.2 The first Data Protection principle is further explained below but compliance with this principle forces us to ask ourselves with each processing operation:

- Why is it necessary to process this personal data?
- Is it lawful?
- Is it fair to the data subject?

4.2.3 **Conditions for Processing Personal Data**

4.2.4 **Schedule 2** of The Act sets out conditions for processing personal data which make the processing lawful. Under Schedule 2 for fair and lawful processing, **one** of the following conditions **must** be met:

(i) The data subject concerned has given his/her consent

(ii) The processing is **necessary** for the performance of, or when entering into, a contract with the data subject:

- This is the case for processing which is considered necessary for the performance of an employment contract and in any other case where the relationship with the data subject is regulated by a contract

- This condition also covers any processing carried out in a pre-contractual situation, which is necessary in order to enter into a contract with the data subject; for example, obtaining and further processing job applicants' personal data

(iii) The processing is **necessary** to comply with any legal obligation imposed on the Council's services:

- A legal obligation may be imposed by any law, such as employment, tax legislation, or any other legislation regulating the activities and the functions

of the Council's Service and their relationship with other public bodies.

(iv) The processing is **necessary** in order to protect the vital interests of the data subject.

- Vital interests are usually taken to mean the protection of data subject's life

(v) The processing is **necessary** for the administration of justice, or, under the provisions of the Freedom of Information (FOI) Act 2000, for the exercise of any functions of the Council; or of any function conferred by or under any enactment or any other public function in the public interest.

- This condition is likely to be most significant for the Council as it may provide a condition for processing personal data in connection with any of the administrative or procedural functions of the Council. However, in each case both the specific function, and why the processing is absolutely necessary in connection with that specific function must be defined. It should not be relied upon more than strictly necessary

(vi) The processing is **necessary** for the legitimate interests of the Council's Service, or the third party or parties to whom data are disclosed, providing the rights and freedoms or legitimate interest of the data subject are not prejudiced.

- The use of this provision in all cases must be balanced by consideration of the legitimate interests of the data subject. If it is intended to rely upon the condition, the advice of the Data Protection officer **must** first be sought.

4.2.5 Conditions for Processing Sensitive Personal Data (Schedule 3)

4.2.6 The Act defines certain personal data as "Sensitive Personal Data" (see paragraph 2.3 above).

4.2.7 If the information concerned is Sensitive Personal Data, Schedule 3 of The Act says that it can only be processed if **one** of the following conditions is also **met**:

(i) The subject has given **explicit** (usually written) consent to the processing

(ii) The processing is **necessary** for exercising or performing any right or obligation, which is conferred or imposed by law on the Data Controller in connection with employment

(iii) The processing is **necessary** in order to protect the vital interests of the subject or another person. The processing is carried out in the course of its legitimate activities by anybody or association which is not for profit and exists for political, philosophical, religious or trade union purposes, and

- is carried out with proper safeguards
- relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes
- does not involve disclosure of the personal data to a third party without the consent of the data subject

(iv) The information contained in the personal data has been made public as a result of steps taken deliberately by the data subject

(v) The processing is **necessary** for, or in connection with any legal proceedings, for obtaining legal advice or for establishing or defending legal rights

(vi) The processing is **necessary**:

- For the administration of Justice
- Under provisions of the Freedom of Information Act 2000
- For the exercise of any function conferred under any enactment for a Government Department.

(vii) The processing is **necessary** for medical purposes and is undertaken by:

- A Health Professional (as defined in Section 69 of The Act
- A person who owes a duty of confidentiality, which is equivalent to that which would arise if that person were a Health Professional.

(viii) The processing is of data about racial or ethnic origin which is needed for ethnic monitoring and is carried out with proper safeguards.

4.2.8 How to obtain the Data Subject's Consent

4.2.9 Everyone in the Council should take into account the following when seeking consent for the processing of personal data from Data Subjects:

- Consent must be informed
- The Data Subject has to be informed as to what he/she is asked to consent to, e.g. who will hold the personal data, for what purposes, who will the data be passed to etc
- Consent must be specific
- A sweeping consent is not valid. Consent cannot be sought for any unspecified processing, but has to relate to particular processing operations, particular uses of data and particular recipients

- Consent must be freely given

- Data Subjects must not be forced into consenting to any processing operations

- Consent should be obtained, where possible, in writing

- Where consent is obtained over the telephone, it must be properly documented

- Where possible, consent should be obtained at the same time as the notice to the Data Subject about processing is made

- In some circumstances (provided Sensitive Personal Data is not involved) it would be enough to seek consent in an opt out form, inviting the Data Subject to demonstrate their disagreement by filling in a specified box, or writing to a designated person

- In cases of processing operations involving Sensitive Personal Data, data subjects have to give their **explicit consent in writing**

- Where applicable, a consent form should be included in a contract with the Data Subject, such as an employment contract

- Data subjects may revoke the consent at any time

4.3 The Second Principle - Personal Data shall be obtained only for defined purpose(s)

4.3.1 Personal Data must be obtained and processed for one or more lawful purposes, which are specified as appropriate in:

- Any notification to the Information Commissioner
- A Data Protection Notice to the Data Subject concerned

4.3.2 In other words, all members of staff have a duty to ensure that Personal Data, which has been obtained for a particular purpose, is further used, disclosed or otherwise processed in accordance with and within the limits of that purpose. This becomes particularly important in situations where personal data are passed on or shared between different departments.

4.3.3 For example:

- Personal Data obtained in the process of recruitment and employment with the Council should be used only in a way which is compatible with recruitment and employment purposes

- Personal Data which the Council services obtain from advisers for the purpose of assisting in an enquiry or review should only be used for that sole purpose and not be further held and processed for some other reason

4.3.4 Use of Existing Personal Data for New Purposes

4.3.5 There may be cases where the Council's legitimate needs require the use of personal data held already by the Council for new purposes, either within the same or another department. These new uses and processing of personal data may not have been envisaged at the time when personal data was obtained and processed in the first instance. In order to comply with the Second Data Protection Principle, the Council's service has to treat the new use of existing personal data as new processing altogether. This means that, in practice:

- Such new processing has to fulfil one of the conditions for fair and lawful processing of personal data as described in paragraph 4.2 above

- The Data Subjects concerned have to be informed of the new planned use of their personal data by the Council and given an opportunity to object

4.3.6 Disclosures of Personal Data

4.3.7 All members of staff must observe the rules below when passing on to others personal data held and processed by the Council. These rules apply in situations where personal data are disclosed:

- to another department
- office
- committee within the Council
- to a third party, i.e. a contractor outside the Council Service

4.3.8 Any disclosure of personal data like any other processing operation has to fulfil one of the conditions for fair and lawful processing as explained when dealing with the First Principle above. Where disclosure/access to personal data is given to a third party, for example, to I.T contractors, the Council's Non-Disclosure Agreement must be applied (see Non-Disclosure Agreement at Appendix 1)

4.3.9 Any disclosure of personal data has to be compatible with the purpose for which that personal data has been obtained and further processed by the Council. It is essential to take into account the intended uses of personal data by a person to whom data has been passed.

4.3.10 For example, the Second Data Protection Principle would be contravened if the Council Service obtained personal data from its employees for employment purposes and passed it to a travel agency, health club or an insurance company for marketing of their products and/or services.

4.4 **Third Principle - Personal Data shall be adequate, relevant and not excessive**

4.4.1 Everybody in the Council should ensure that when obtaining personal data from Data Subjects and other sources only the minimum information necessary is actually collected and recorded. Personal data **must not** be collected because the data **may** prove useful in the future. There must always be a legitimate reason for

obtaining and further processing personal data about the Data Subject.

4.4.2 The Data Controller should continually monitor compliance with this principle, which has obvious links with the fourth and fifth principles.

4.4.3 As soon as a purpose of processing ceases to exist, or changes, the item(s) of data which relate only to that purpose have to be deleted.

4.4.4 The Data Controller should consider for all data:

- The number of individuals on whom information is held
- The number of individuals by whom it is used
- The nature of the personal data
- The length of time it is held
- The way it was obtained
- The possible consequences for individuals of the holding or erasure of the data
- The way in which it is used
- The purpose for which it is held

4.4.5 For example:

On occasions, Managers may hold data on absence, performance or relevant experience. However, this could only be justified where there is a real need for those managers/officers to hold such personal data. Any irrelevant material should be deleted from the employees file.

4.5 **The Fourth Principle - Personal Data shall be accurate and, where necessary, kept up-to-date.**

4.5.1 The Council is required to take reasonable steps to ensure accuracy of information.

4.5.2 This principle, which refers to keeping personal data up-to-date, is qualified. Updating is only required "where necessary". The purpose for which the data are held or used will be relevant in deciding whether updating is necessary. For example, if the data are intended to be used merely as an historical record of a transaction between the Data Controller and the Data Subject, updating will be inappropriate. However, it is important that the data reflect the Data Subject's current circumstances, if the data are used to decide whether to grant credit, confer, or withhold some other benefit. In those cases, either step should be taken to

ensure that the data are kept up-to-date, or when the data are used, account should be taken of the fact that circumstances may have changed.

4.5.3 A Data Controller will need to consider the following practice:

- Is there a record of when the data was recorded or last updated?
- Are all those involved with the data – including people to whom they are disclosed as well as employees of the Data Controller – aware that the data do not necessarily reflect the current position?
- Are steps taken to update the personal data – for example, by checking back at intervals with the original source or with the Data Subject? If so, how effective are the steps?
- Is the fact that the personal data are out of date likely to cause damage and/or distress to the Data Subject?

4.6 **The Fifth Principle -** "Personal Data shall not be kept longer than is necessary for the purpose(s) for which it has been processed.

4.6.1 Everyone in the Council must ensure that personal data are kept only as long as data remain necessary for the purpose(s) for which data have been obtained and processed in the first place.

4.6.2 To comply with this principle all departments will need to review their personal data regularly to delete the information which is no longer required for their purposes. **(see paragraph 7 below – Data Management)**

4.6.3 Statutes may make specific provision relating to the retention of certain categories of data, for example, the Police and Criminal Evidence Act 1984 and Limitation Act 1980. In addition, recommendations in regard to certain information can be found in the CCTV Code of Practice published by the Commissioner which contains guidance on retention periods of recorded material.

4.6.4 If personal data have been recorded because of a relationship between the Council and the Data Subject, the need to keep the information should be considered when the relationship ceases to exist. For example, the Data Subject may be an employee who has left the employment of the Council.

4.6.5 Bad housekeeping is no excuse for holding on to personal information for longer than strictly necessary. It must be decided how long all forms of personal data are going to be kept and this period must be documented**.** The Council's Data Protection officer must also be told of these retention periods.

4.7 **Sixth Principle -** "Personal Data shall be processed in accordance with the rights of Data Subjects under this Act".

4.7.1 A person will contravene this principle if, but only if:

(i) He/she fails to supply information pursuant to a subject access request under Section 7 of The Act (See section 5 of this guidance for information about subject access requests); or

(ii) He/she fails to comply with Notices given under the following provisions of The Act:

- The right to prevent processing causing damage or distress
- The right to prevent processing for the purpose(s) of direct marketing; or
- The rights in relation to automated decision making

4.7.2 This includes the right to be told that processing of their personal information is being carried out and the right to have information which is wrong rectified, blocked or erased.

4.8 **The Seventh Principle - Personal Data shall be protected by appropriate technical and organisational or data security measures. (See the Council's ICT Security Policy)**

4.8.1 The Council acts as custodian of the data subjects personal data and therefore has a responsibility to see that sufficient precautions are taken to avoid:

- Unauthorised or unlawful processing of personal data
- Accidental loss, disclosure or destruction of and damage to personal data

4.8.2 In determining appropriate security measures, account should, in particular, be taken of:

- The need to provide for different levels of security according to risks involved in various processing operations

- The nature of personal data
- The state of technological development

4.8.3 The following basic safeguards should therefore be applied by all staff:

- **Manual Files** – All cabinets holding manual records and containing personal data are to be locked outside of office hours and keys properly secured. Personal data must never be left on an unattended desk
- **Electronic Files** – Access to electronic files containing personal data must be via username and password or by restricting physical access to any stand-alone computer. Passwords must meet the Council's standards and must be regularly changed and not given to anyone. In the case of sensitive data, all electronic files should, where reasonably possible be encrypted (Please read in conjunction with the ICT Security Policy – link to include)
- **Website and intranet** – Authorised users must access the website or intranet via username and password. Passwords should not be available to unauthorised staff
- **External Agencies** – Where external agencies process personal data on behalf of South Kesteven District Council, the Council must have guarantees by way of third party agreements (see Appendix 1) that the securities measures the agency has in place are appropriate
- **Computer Screens** – Don't let unauthorised persons see personal data on your screen unless they have a valid reason to do so.

4.8.4 This document must be read in conjunction with the Council's Data Security Policy and staff must work within a general Data Protection Security Framework:

4.8.5 **The Security Framework**

- The responsibility is on all staff to adhere to their duty of confidence and comply with full stat**u**s security procedures. If a course of action is unclear, they must ask managers and if it is unclear to them, they must ask Departmental Data Protection Representatives or the Data Protection Officer

- managers must accept responsibility for ensuring that staff are aware of and comply with security procedures

- managers must adopt measures to ensure the integrity of staff through selection, training, supervision and motivation. This includes non-permanent staff permitted access to personal data

- in areas where personal data are processed access, controls, both physical and logical, must be implemented and audit trails put in place

4.9 **The Eighth Principle -** Personal Data shall be adequately protected when transferred to countries outside the **European Economic Area (EEA).**

4.9.1 This principle limits the transfer of personal data to countries within the EEA. The transfer of personal data outside the EEA is not permitted unless the country has an adequate level of protection.

4.9.2 You may think this is not an issue, however the internet is available worldwide meaning the information you put on the internet is also available worldwide. Also, it is becoming more common for organisations to have data taken to corporate visits abroad (especially laptop computers), or to have help desk or IT support functions situated in another time zone.

5. Subject Data Access Request

5.1 Every Data Subject may demand access to all personal data held and processed about him/her. Access to the data should enable the individual to check the accuracy and to ensure that they have been collected, held and otherwise processed in accordance with the law.

5.2 What are our duties?

5.2.1 When an individual makes an access request, the Council has to provide the following information in response to such a request:

(i) Whether that individual's personal data are processed by the Council

- both automated data (e.g. all files held on a personal computer or server, CCTV coverage, email and internet files) and data held in manual files (e.g. personal or case files) must be considered

- data need not be used; it is enough that they are held by the Council

(ii) Where data are processed by the Council the description of the data, purposes for which data are, or will be processed and recipients to whom data are or may be disclosed

(iii) Communication of such data in an intelligible form and any available information on the sources of those data. Copies of paper information should normally be provided.

- the individual requesting access has to be able to understand the data communicated to him/her. Any coded or otherwise unintelligible data has to be presented in an understandable format

- the sources of data have to be included in the information to the individual only where the Council knows of the sources or personal data relating to that individual

- sometimes giving information about a source or data would mean disclosing personal data of another individual e.g. by identifying him/her as the source of data. In these cases, any such personal data identifying an individual as the source of data may have to be omitted from the information supplied to the Data Subject concerned

5.3 Procedure

1. Requests received:

   Applicants must complete, sign and date "Subject Access Information Request Form" available on the South Kesteven District Council website

2. The Applicants pay a £10 supply fee

3. The persons making the Subject Access Request must provide original proof of identity (list on form) "shown in person" at the Council Offices to an officer – photocopy retained of identity e.g. passport/photograph

4. The request must be sent to Legal Services to be processed. This will involve:

- entry of request on to a central register with date application received; forty calendar days deadline; completion date; name of requester; address; description of request; exemption details; outcome details)

- consultation with the relevant service area(s) to search for personal information required and collate (within forty-day timescale)

- receipt of copy documents produced. Keep a copy of all information to be supplied and retain copies of any information that has been redacted (i.e. personal details of "another" **must** be removed before the information is provided to the Data Subject requester)

- contact the Data Subject Requester inviting them to come into the offices to collect the information in person bringing with them proof of identity – ask Data Subject Requester to sign and date a receipt for the information handed over

5. If requests are made by a third party i.e. "Shelter" on behalf of a Data Subject, a "Form of Authority" must be provided by "Shelter" which has been completed and signed by the Data Subject to enable "Shelter" to request information on the Data Subject's behalf. (Housing Solutions supply this information by Recorded Delivery to "Shelter").

6. A Data Controller must comply with a Subject Access Request promptly, in other words as quickly as he can, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of:

    - the information required to satisfy himself as to the identity of the person making the request to enable him to locate the information which that person seeks

    - the fee

5.4 Can we claim any exemptions from the Right of Access?

5.4.1 The Council should make its best efforts to supply the Data Subject with the necessary and requested data in response to an Access Request. The Policy of the Council is to promote

transparency and openness in personal data processing operations. Consequently, exemptions to the Right of Access should be relied upon only in exceptional circumstances.

5.4.2 In general, exemptions should be claimed where disclosing personal data to the Data Subject in a response to the Access Request would prejudice the interests and operations of the Council.

5.4.3 The Council is not obliged to respond to a Data or Subject Access Request in the following circumstances:

(i) if the request has not been made in writing

(ii) if the Council has not been supplied with reasonably requested information about the Data Subject identity and the location of the data

(iii) if giving access to the Data Subject will lead to a disclosure of personal data of another individual. However, access to such personal data may be allowed where:

- the other individual has consented to such disclosure or
- it is reasonable to supply the data without the consent of that other individual, bearing in mind any duty of confidentiality owed to that individual, any steps taken to seek and obtain the consent, and the results of such steps

5.4.4 If the Council has already complied with a previous, identical or similar request or access from the same Data Subject and a reasonable period has not elapsed since that previous request:

(i) assessing whether the period from the previous request is reasonable account should be taken of the nature of data, the purpose of processing and the frequency with which data are altered

(ii) where personal data and records are frequently amended and altered, or personal data belongs to the category of sensitive data (see paragraph 2.3 above), or the purpose of processing has changed, then the repeated Subject

Access Request may not be unreasonable and should be complied with.

5.4.5 **Prevention of Processing Causing Damage or Distress (Section 10)**

5.4.6 If that individual believes that a Data Controller is processing personal data in any way that causes, or is likely to cause, substantial and/or unwarranted damage or substantial unwarranted distress to them or to another, Section 10 of the Act provides that the individual has the right to send a Notice to the Data Controller requiring him/her within a reasonable time, to stop the processing (the "Data Subject Notice").

6. Exemptions and Modifications

6.1 The Exemptions

6.1.1 The Exemptions cannot easily be categorised into classes which ensure the same type of exemption. However, a number of categories of exemptions consist of, or include, an exemption from one or other of the following categories or provisions:

6.1.2 **"The Subject Information Provisions"**

6.1.3 **These are**

- The requirement under the first data protection principle to process data fairly, in so far as it requires the data controller to give the data subject information about the purpose for which the data is required, and any other information which the data subject ought to know

- Section 7 – the data subjects rights to access – (see part 5 above)

6.1.4 **Other exemptions which may be applicable are as follows:**

6.1.5 **Crime and Taxation (Section 29)**

6.1.6 Certain exemptions apply to data required for:

- preventing or detecting crime
- prosecutions
- assessing liability to any tax (including Council Tax and NNDR)
- collecting any such tax

6.1.7 Data required for these purposes is exempt from:

- the requirement under the First Data Protection Principle to process data fairly and lawfully (but not from the need to meet one of the conditions in schedule 2 and, where the data is sensitive persona1 data schedule 3)
- the data subjects right to access under section 7
- the non-disclosure provisions

6.1.8 This is of course highly relevant to the exchange of information between prosecuting and taxation authorities.

6.2 Health and Safety

6.2.1 Certain exemptions apply in relation to any of the Council's regulatory functions which:

- relate to health and safety and welfare at work
- protect the public against risks to their health and safety caused by anyone in the course of their work

6.2.2 They therefore apply, for example, to the Council's environmental health function and building control.

6.2.3 Personal data processed to carry out these functions is exempt from the subject information provisions where applying them would prejudice the Council in carrying out its regulatory functions.

6.3 Research, history and statistics

6.3.1 It is unlikely that the Council processes any data for purely historical purposes, but it certainly carries out research and compiles statistical information.

6.3.2 These are exemptions relating to data processing for these purposes which apply provided that data:

- is not used to determine individual cases
- is not processed in a way which causes substantial damage or distress to the data subject

6.3.3 If these conditions are met:

- data obtained for other purposes may be further processed for research or statistical purposes

without contravening the Second Data protection Principle
- data may be kept indefinitely, notwithstanding the fifth data Protection Principle
- data exempt from the data subject's right of access, provided that they cannot be identified from the research or statistics

6.3.4 Data held for research purposes must not be processed for any other purposes. However, disclosing data will not be regarded as "processing it for another purpose" if the disclosure is made:

- for research purposes only
- to the data subject or anyone acting for him/her
- at the request of the data subject, or anyone on his/her behalf
- in circumstances where the person making the disclosure has reasonable grounds for thinking that one of the above applies.

6.4 Information the authority is statutory obliged to make available to the public

6.4.1 Where the authority is obliged to make personal data available to the public under any Act of Parliament or Statutory Instrument, the data is exempt from:

- the subject information provisions
- the Fourth data Protection Principle (accurate and kept up to date)
- the data subjects right to apply to the Court for an Order rectifying blocking or erasing or destroying the data
- the non-disclosure principles.

6.5 Disclosure required by law

6.5.1 Personal data is exempt from the non-disclosure provision where the disclosure is required:

- under any act or Statutory Instrument
- by common law
- by order of the Court

6.5.2 Personal data is also exempt from the non-disclosure provisions where the disclosure is necessary:

- in legal proceedings

- for obtaining legal advice
- for establishing, exercising or defending legal rights

6.6 **References**

6.6.1 References given in confidence are exempt from Section 7 of the Act (i.e. their contents need not be disclosed to the subject), if they are given for the purposes of:

- education, training or employment
- the appointment of the data subject to any office
- The provision by the data subject of any service

6.6.2 Oddly, the exemption does not apply once a reference is in the hands of the recipient as the recipient on receipt of a subject access request must disclose the content of the reference.

7. MANAGEMENT OF DATA PROTECTION COMPLIANCE & POLICY

7.1 Who to go to for further information and replies?

7.1.2 If you have any queries or problems in interpreting and/or implementing this Policy, and whenever in doubt about Data Protection Practice and Compliance, please contact:

7.1.3 South Kesteven District Council's Protection Officer: Andy Nix extn. 6433 and Lucy Youles extn. 6105

For the relevant Departmental Representatives

Executive Manager – Commercial
Executive Manager - Development and Growth
Executive Manager - Property
Chief Executive
Executive Manager - Corporate
Executive Manager - Environment
Business Manager - Business Transformation

8. Review of the Policy

8.1 The Council's Data Protection Policy must be reviewed at least annually.

8.2 The scope of any such revision, must take account of, in particular:

(i) any changes to the United Kingdom Data Protection Legislation which may have occurred
(ii) any change in or additional interpretation and guidance given by the Information Commissioner
(iii) any change in current practises within the Council, as well as, any new requirements that may involve processing of personal data on a new basis

8.3 **Consulting with Council's Departmental Representatives**

8.3.1 Before any new plan, campaign or activity involving obtaining and further processing of personal data by the Council commences, the relevant managers must inform, consult and involve in the process the Departmental Representative.

8.3.2 **Managers must consider the following:**

- the conditions (grounds for processing personal data)
- the necessity of obtaining consent in some cases and the form and content of such consent
- the relevance and adequacy of personal data collected from individuals
- whether notification to the Information Commissioner might be required

9 How does Freedom of Information (FOI) Fit With Data Protection?

9.1 A request by individuals for information about themselves will be exempt under Freedom of Information Act and will continue to be handled under Data Protection. If someone makes a request for information about another living individual, this will be handled under the Freedom of Information Act 2000, but certain Data Protection considerations will still apply, for example we will not have to provide the information if the disclosure will breach the Data Protection Principles. If we decide to disclose information then we will usually notify the individual taking into account their wishes, although, we are not always bound by the views of the individual.

10. Co-working, Hot Desking and Home working

10.1 Co-working, hot desking and working from home presents some security issues. Officers and Members of the Council working in

these situations must comply with the Information Security and Records Management Protocol for the purposes of co-location, hot desking and home working (see APPEDNIX 2)

11. Personal Data and Elected Members

11.1 The provisions of the data protection Act and the Council's Data Protection Policy apply equally to elected members as it does employees of the Council.

11.2 Before making any disclosures of personal data to elected members local authorities must ensure that they have listed them as recipients of personal data in their data protection notifications.

11.3 Disclosures to the Elected Member as a member of the Council

11.3.1 Disclosures of personal data may be made to an elected member if access to and use of that data is necessary for him/her to carry out official duties. The member is *NOT* required to have his or her own data protection notification and is, effectively, in the same position as an employee.

11.4 Use of personal data by elected members

11.4.1 When considering whether it is permissible to make use of personal data for any particular purpose, elected members must first consider the context in which that information was collected, and who is the data controller for that data. For example:

(i) information, which is held by the local authority, may not be used for political or representational purposes unless the individuals to whom the data relate (the "data subjects") have agreed. Thus it would not be permissible to use a list of users of a particular Council Service (Arts Centres) for electioneering purposes (e.g. a campaign against the closure of local art centres) without the consent of those individuals

11.4.2 Similarly it would not be permissible to use personal data to which the elected member had access in an official capacity, as a member of the Planning Committee, in order to progress objections on behalf of a local resident unless all the individuals concerned had consented.

11.4.3 When campaigning for election, candidates may make use of personal data held by their parties such as mailing list and of

personal data, which they hold as elected members. For instance it would be permissible to seek support from local residents whom the candidate has assisted in the past as a councillor. It would not, however, be permissible to disclose the details of those local residents to the party without consent.

12. Offences under the Act

12.1 Who can bring proceedings?

12.1.1 The Information Commissioner has been established to supervise and enforce the application of the Data Protection Act. The Commissioner has considerable powers.

12.1.2 The Commissioner may:

- hear and consider complaints from individuals
- enter the Data Controller's premises and carry out an inspection, in a case of a suspected breach of the data protection principles
- serve an information notice requesting information in relation to a suspected breach of the data protection principles
- serve an enforcement notice of breaches of the data protection principles, requiring the Data Controller to comply with the principle in question

12.2 Possible Criminal Penalties

12.2.1 It is a criminal offence to breach certain provisions of the act and employees/members of the Council may be individually liable to prosecution if they obtain/or disclose unlawfully personal data without the Data Controller's consent, for example, it is an offence for a person, knowingly of recklessly, without the consent of the data controller to:

- obtain or disclose personal data or the information contained in personal data
- disclose or pass on to another person the information contained in personal data

12.3 Sanctions

12.3.1 A person found guilty of an offence may be sentenced in the Magistrates' Court to a fine not exceeding the statutory maximum (currently £5,000), or where the offences, as the example given above, falls into an "either way offence", the matter can be dealt with in the Crown Court (on indictment) where the fine is unlimited.

12.4 Compensation for damage and distress

12.4.1 Any individual has a right to sue for compensation when she/he suffers damage as a result of a breach by the Data Controller of the Act.

APPENDIX 1

THIS AGREEMENT dated …… 20.... is made **BETWEEN:**

(1) South Kesteven District Council (the Council) and

(2) …….. a company registered in (England) under number……..

whose registered office is at ……
(the Contractor)

BACKGROUND

The parties wish to …….. and this is likely to involve them disclosing Confidential Information to each other.

1. DEFINITIONS

In this Agreement the following expressions have the meaning set opposite:

This Agreement	this document, as amended from time to time in accordance with clause and 5.7
A Business Day	Monday to Friday (inclusive) except bank or public holidays in England
Confidential Information	each party's personal data information including any Intellectual Property and Know-how disclosed by that party to the other for the Specified Purpose
A Group Company	any undertaking which is, on or after the date of this Agreement from time to time, a subsidiary undertaking of the Company, a parent undertaking of the Company or a subsidiary undertaking of a parent undertaking of the Company, as those terms are defined in section 258 of the Companies Act 1985
Intellectual Property	patents, trade marks, service marks, registered designs, copyrights, database rights, design rights, confidential information, applications for any of the above, and any similar right recognised from time to time in any jurisdiction, together with all rights of action in relation to the infringement of any of the above
Know-how	unpatented technical information (including, without limitation information relating to inventions, discoveries, concepts, methodologies, models, research, development and testing procedures, the results of experiments, tests and trials, manufacturing processes, techniques and specifications, quality control data, analyses, reports and submissions) that is not in the public domain
Personal data	data defined as personal in the Data Protection Act 1998

the Proposed Project: .....

the Specified Purpose: .....

2 CONFIDENTIALITY

2.1 Neither party will disclose to any third party, nor use or process for any purpose except the Specified Purposes, any of the other party's Confidential Information.

2.2 Neither party will be in breach of any obligation to keep any Confidential Information confidential or not to disclose it to any other party to the extent that any disclosure:

2.2.1 is not in breach of the Data Protection Act 1998

2.2.2 is known to the party making the disclosure before its receipt from the other party, and not already subject to any obligation of confidentiality to the other party

2.2.3 is or becomes publicly known without any breach of this Agreement or any other undertaking to keep it confidential

2.2.4 has been obtained by the party making the disclosure from a third party in circumstances where the party making the disclosure has no reason to believe that there has been a breach of an obligation of confidentiality owed to the other party

2.2.5 has been independently developed by the party making the disclosure

2.2.6 is disclosed pursuant to the requirement of any law or regulation (provided, in the case of a disclosure under the Freedom of Information Act 2000, none of the exceptions to that Act applies to the information disclosed) or the Order of any Court of competent jurisdiction, and the party required to make that disclosure has informed the other, within a reasonable time after being required to make the disclosure, of the requirement to disclose and the information required to be disclosed

2.2.7 is approved for release in writing by an authorised representative of the other party

2.3 The Company will not be in breach of any obligation to keep any of the Council's Confidential Information confidential or not to disclose it to any third party by making it available to any Group Company, or any person working for or on behalf of the Company or a Group Company, who needs to know the same for the Specified Purpose, provided it is not used except for that purpose and the recipient undertakes to keep that information confidential.

2.4 If the Council receives a request under the Freedom of Information Act 2000 to disclose any information that, under this Agreement, is the Company's Confidential Information, it will notify the Company and will consult with the Company. The Company will respond to the Council within 10 days after receiving the Council's notice if that notice requests the Company to provide information to assist the Council to determine whether or not an exemption to the Freedom of Information Act applies to the information requested under that Act provided that nothing in this Agreement will prevent the Council from complying with its obligations under the Freedom of Information Act 2000.

2.5 The Company will at all times during the term of this Agreement comply with the Data Protection Act 1998 and the Council's Data Protection Policy and Information Security Policy.

3 INTELLECTUAL PROPERTY

3.1 Nothing in this Agreement grants any licence or right, beyond that required for the Specified Purpose, under any patent, copyright, trade secret or other Intellectual Property.

3.2 Neither party will remove any proprietary, copyright, trade secret, confidentiality or other notice from any of the other's Confidential Information.

4 TERM

4.1 Subject to clause 2.1, this Agreement will continue indefinitely despite the conclusion of the discussions between the parties concerning the Proposed Project for the term of the Contract provided all restricted inputs of data information have been destroyed by the Contractor.

4.2 To the extent that the terms of this Agreement conflict with any agreement entered into between the parties for carrying out the Proposed Project, the terms of the agreement for the Proposed Project will prevail, but only to the extent necessary to resolve that conflict.

4.3 At the conclusion of the discussions about the Proposed Project, unless the parties enter into an agreement for the carrying out of that project, each of the parties will, at the other's request:

4.3.1 return or destroy the other's Confidential Information in its possession, custody or control

4.3.2 confirm in writing that the above has been done

5 GENERAL

5.1 **Notices:** Any notice to be given under this Agreement must be in writing, may be delivered to the other party by any of the methods set out in the left hand column below, and will be deemed to be received on the corresponding day set out in the right hand column:

Method of service	Deemed day of receipt
By hand or courier	The day of delivery
By prepaid first class post	The second Business Day after posting
By recorded delivery post	The next Business Day after posting
By fax (provided the sender's fax machine confirms complete and error-free transmission of that notice to the correct fax number)	The next Business Day after sending or, if sent before 16.00 (sender's local time) on the Business Day it was sent

The parties' respective representatives for the receipt of notices are, until changed by notice given in accordance with this clause as follows:

For the Council:	For the Company:
Name:	Name:
Address:	Address:
Fax number:	Fax number:

5.2 **Headings:** The headings in this Agreement are for ease of reference only; they do not affect its construction or interpretation.

5.3 **Assignment:** Neither party may assign or transfer this Agreement as a whole, or any of its rights or obligations under it, without first obtaining the written consent of the other party. That consent may not be unreasonably withheld or delayed.

5.4 **Illegal/unenforceable provisions:** If the whole or any part of any provision of this Agreement is void or unenforceable in any jurisdiction, the other provisions of this Agreement, and the rest of the void or unenforceable provision, will continue in force in that jurisdiction, and the validity and enforceability of that provision in any other jurisdiction will not be affected..

5.5 **Waiver of rights:** If a party fails to enforce, or delays in enforcing, an obligation of the other party, or fails to exercise, or delays in exercising, a right under this Agreement, that failure or delay will not affect its right to enforce that obligation or constitute a waiver of that right. Any waiver of any provision of this Agreement will not, unless expressly stated to the contrary, constitute a waiver of that provision on a future occasion.

5.6 **No agency:** Nothing in this Agreement creates, implies or evidences any partnership or joint venture between the parties, or the relationship between them of principal and agent. Neither party has any authority to make any representation or commitment, or to incur any liability, on behalf of the other.

5.7 **Entire agreement:** This Agreement constitutes the entire agreement between the parties relating to its subject matter. Each party acknowledges that it has not entered into this Agreement on the basis of any warranty, representation, statement, agreement or undertaking except those expressly set out in this Agreement. Each party waives any claim for breach of this Agreement, or any right to rescind this Agreement in respect of any representation which is not an express provision of this Agreement. However, this clause does not exclude any liability which either party may have to the other (or any right which either party may have to rescind this Agreement) in respect of any fraudulent misrepresentations or fraudulent concealment prior to the execution of this Agreement.

5.8 **Amendments:** No variation or amendment of this Agreement will be effective unless it is made in writing and signed by each party's representative.

5.9 **Third parties:** No one except a party to this Agreement has any right to prevent the amendment of this Agreement or its termination, and no one except a party to this Agreement may enforce any benefit conferred by this Agreement, unless this Agreement expressly provides otherwise.

5.10 **Governing law:** This Agreement is governed by, and is to be construed in accordance with, English law. The English Courts will have exclusive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement, except that either party may bring proceedings for an injunction in any jurisdiction.

5.11 **Escalation:** If the parties are unable to reach agreement on any issue concerning this Agreement or the Project within 14 days after one party has notified the other of that issue, they will refer the matter to …… in the case of the Council, and to …… in the case of the Company in an attempt to resolve the issue within 14 days after the referral. Either party may bring proceedings in All personal data as defined by the Data Protection Act, information and other data received by the contractor from the Council throughout this contract will be confidential information. The contractor shall not make use of any information or data other than the purposes for which it was provided and for no other purpose.

Each party will indemnify the other against the cost of all third party actions, claims and/or demands including costs, charges and expenses (including legal expenses on an indemnity basis) brought against the other party as a result of any breach of this Agreement and/or any failure to comply with the legislation referred to in this Agreement

In witness of this Agreement the parties have signed this document on the above date

Signed by
Print name (authorised signatory)

On behalf of:

Witness
Print name
Address

Signed by (authorised signatory)
Print name
On behalf of

Witness
Print name
Address

APPENDIX 2

Information security and records management protocol for the purposes of co-location, hot desking, mobile and home working

All individuals working on behalf of the Council have a statutory duty under the Data Protection Act to protect information they create, hold and/or process which identifies an individual and the service received. This includes paper or electronic information relating to customers (service users), employees or commercially sensitive information.

Officers and Members of the Council must follow the policies, procedures, and this protocol at all times and specifically for the purposes of co-location hot desking and home working to ensure information is only shared on a need to know basis and kept secure at all times.

Clear desk

Paper information must be restricted to authorised users. Desks must be cleared of information when leaving the office, or in home working environment, even for a short period of time to ensure unauthorised Officers or visitors to your home do not have sight or access to the personal information of service users.

Passwords and electronic system access

Never disclose or share usernames and passwords for access to electronic systems or networks. Computer and laptop screens must be locked when leaving unattended (even when having a short break) and must be shut down at the end of the day. When home working laptops must be locked away when not in use. Files must not be copied from work drives to local drives (your home PC). Personal data must not be stored on any device (including removable media such as USB sticks) that does not have corporately approved encryption. Taking home paper or electronic files creates a risk of loss. It also means the files are not accessible to other members of staff. Controls in the office must include a signed log when you are removing and returning files to the office.

Home Visits

When carrying out home visits only those documents relevant to that service user should be taken into their home and all others documents must be kept locked out of sight in the boot of the car.

Confidentiality

Think about the level of information required for discussions, for example is it necessary to use names and other identifying personal information. This could relate to face to face discussion, telephone conversations and correspondence. (There may be occasions when it would be advisable to use a private designated meeting room/area for more sensitive conversations. Officers of the Council may occupy a desk within any area of the Council's Offices or share office space with other organisations. In those circumstances Officers may overhear conversations where personal information relating to a service user is discussed. In these circumstances, Officers must treat that information in the strictest confidence and not share that information with third parties.

Sharing Information

Think carefully before sharing information and whether the person requesting has the right to share the information under the Data Protection Act or other relevant legislation. Consider who is asking? Why the information is needed? How it would be used? Refer to the Council's Data Protection Policy and Information Governance for guidance.

Printing

Secure print functions must be used (where available) or collect what you print immediately. Never print records containing a service users (member of the publics) details in a public place. Please consider the information you print could contain information relating to employees, family, friend or next door neighbour, access must be restricted to information.